UNIVERSITY OF EDUCATION, WINNEBA

COLLEGE OF TECHNOLOGY EDUCATION, KUMASI

A SECURE IOT-BASED SMART DAYCARE IMPLEMENTATION IN GHANA. A CASE STUDY OF LAMBUSSIE DISTRICT.

INUSAH AN-ICHIE

DECEMBER, 2021

UNIVERSITY OF EDUCATION, WINNEBA

COLLEGE OF TECHNOLOGY EDUCATION, KUMASI

A SECURE IOT-BASED SMART DAYCARE IMPLEMENTATION IN GHANA. A CASE STUDY OF LAMBUSSIE DISTRICT.

INUSAH AN-ICHIE

(7191040021)

A Dissertation in the Department of Information Technology Education, Faculty of Technical Education, submitted to the school of Graduate Studies, in Partial Fulfilment of the requirements for the award of the degree of Master of Science (Information Technology Education) in the University of Education, Winneba-Kumasi

DECEMBER, 2021

DECLARATION

STUDENT'S DECLARATION

I, INUSAH AN-ICHIE, declare that this dissertation, with the exception of quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my own original work, and it has not been submitted, either in part or whole, for another degree elsewhere.

SIGNATURE: ……

DATE: ……

SUPERVISOR'S DECLARATION

I hereby declare that the preparation and presentation of this work was supervised in accordance with the guidelines for supervision of thesis as laid down by the University of Education, Winneba.

PROF. EBENEZER BONYAH

SIGNATURE: …….

DATE: ……

DEDICATION

This thesis is in Memory of my late father, An-ichie Batorwie for the need to educate me and from whom I learnt that hard work pays. My brothers (Navei Ibrahim, late Hon. Bayirga Harunah) and my beloved mother, Alhassan Adizatu is forever remembered for whole heartedly sponsoring my Education. Not forgetting my lovely wife, kids and friend, particularly Chakurah Issah for their unflinching support and words of encouragement to making this thesis a success.

ACKNOWLEDGEMENT

This thesis was produced with the immeasurable support of many. I would especially like to first and foremost thank the almighty Allah who by His grace gave me the strength and determination to work on this thesis. I appreciate the academic opportunity and support from the University of Education, Winneba-Kumasi campus now AAMUSTED.

My heartfelt gratitude goes to my supervisor, Prof. Ebenezer Bonyah for his constructive criticisms, brotherly advice, guidance and assistance offered me which in no small way contributed to the success of this thesis.

Special thanks to Mr. Chakurah Issah for your great support, collaboration, useful discussions and overall moral support to help me finish this thesis.

Finally, I want to thank my wife, parents, children and siblings for making my life more pleasant. I thank you very much and may the Almighty Allah replenish all that you have lost because of me and bless you all today and forever more.

TABLE OF CONTENTS

CONTENT **PAGE**

LIST OF TABLES

PAGE

LIST OF FIGURES

PAGE

ABSTRACT

The study was to propose and develop a conceptual model/system for the implementation of IOT based smart daycare system in Ghanaian schools to enhance security of kids and to promote effective teaching and learning. The specific objectives of the study were to find out the extent of need/effectiveness of the smart daycare system implementation, identify potential security threats associated with the smart daycare system and to determine the impact of smart daycare system on the effectiveness of teaching and learning. The research approach used for this study was descriptive. The study setting was Lambussie District of the upper west region in Ghana. The target population was parents and teachers with a sample space of 150 participants. None probability sampling was used. Also, stratified, purposive and convenient sampling techniques were used in the study. Quantitative data was obtained using close-ended questions in the form of questionnaires. Simple percentages, frequency tables, standard deviation, regression analysis and in some cases mean of means were used to present the data. The study also described the architecture of the smart daycare system. Key findings from the study revealed that teachers need the IOT smart daycare system to enable them work independently, automate school processes, improve their ICT competence, monitor student movement, effectively communicate with parents and ensure security of kids when effectively implemented. The study also identified some possible challenges and security threats that may affect the system and possible countermeasures to forestall any security threats. Some of these are; network failure, phishing and spoofing attacks, man in the middle attacks and so on. The system also made significant impact towards improving teaching and learning as revealed by the findings. The implications of these findings are that, more efforts should be made to fully operationalize the smart daycare system in all Ghanaian daycare schools to safeguard the security of kids and promote effective teaching and learning. This also implies that the rate at which kids were kidnapped drastically reduced compared to the open traditional daycare system.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

The Internet of Things (IoT) is already here, thanks to technological advancements and the great desire for acquiring knowledge in the twenty-first century. Smart homes, digital healthcare, smart grids, smart cities, and other Internet of Things (IoT) applications are widely employed in many domains of social production and social living, including healthcare, energy, and industrial automation. While we like the ease and efficiency that IoT provides, new IoT concerns have surfaced that require immediate action.

This chapter provides background information and justifies the research project. The objective and approaches in smart daycare automation security are discussed in this chapter. The chapter is divided into six sections, section 1.0 explains the introduction to the chapter, section 1.1 explains the background to the study. Section 1.2 discusses the statement of the problem, section 1.3 outlines the objectives of the study, section 1.4 discusses the significance of the study, section 1.5 the delimitation. Finally, section 1.6 discusses the organization of the study.

1.2 Background to the Study

There is no universally agreed definition of the Internet of Things. Despite the fact that this word has been used by many other groups, it was first coined by Kevin Ashton, a digital innovation expert. In all the definitions, we have the same idea that the first version of the Internet is about data created by humans, while the second version is about data created by various things, that's why it's called Internet of things (Ashton, 2009).

The Internet of Things (IoT) is a dynamic global network infrastructure comprising physical devices connected to the internet from all over the world, all collecting and sharing data (Shiavi & Behr, 2018j). They opined that IOT ecosystem comprises of web-enabled smart devices that gather, send, and act on data they acquire from their surroundings using embedded systems such as CPUs, sensors, and communication hardware. By connecting to an IoT gateway or other edge device, the IoT devices can share sensor data that is either routed to the cloud for analysis or examined locally. Smart daycare, smart cities, smart healthcare systems, intelligent traffic control lighting, linked vehicles, smart environment monitoring in industries, smart grids, smart metering, water network monitoring, and smart logistics are just a few examples of Internet of Things applications.

The goal of Internet of Things is to expand the capabilities of the first version of the Internet and make it more useful. Users can share information provided by humans, which is stored in databases, as well as information produced by things in the physical world, using the Internet of Things. The Internet of Things is a semi-autonomous network that incorporates many technologies. It establishes connections between individual devices and the network. In the network, there are also controller systems (software and services) that operate as the system's brains, interpreting and utilizing data acquired by connected devices to make decisions and initiate actions from the same or other devices.

Smart daycare is an educational facility for infants that allows them to participate in daily learning and co-curricular activities while simultaneously ensuring their safety and security through surveillance and alarm changes or indications in the event of an intruder. Home security has evolved significantly over the previous century and will continue to evolve in the future

years. In smart childcare system, security is a crucial factor or feature. Smart daycare is a new and rising concept that provides inhabitants with a comfortable, convenient, and safe environment. Standard security systems provide an indicator in the form of an alarm to keep school owners and their property safe from attackers.

The central goal of IoT is to allow us to use the internet to uniquely identify, signify, access, and control things at any time and from any location. The interconnected device networks have the potential to produce a large number of intelligent and autonomous applications and services, which can provide significant personal, professional, and economic benefits.

Smart environments are designed to take advantage of a diverse set of small computational nodes to recognize and deliver customized services to users as they interact and exchange data with the environment. Smart daycare can be created using IoT technology to bring intelligence, comfort, and to improve the quality of our lives. It is now feasible to remotely access and control the electrical gadgets installed in a school compound via the Internet of Things from anywhere in the world. Security guards at a smart daycare, for example, will automatically determine when a parent brings his child to the center, what the child is doing at any given time, control the air conditioning system, smart TVs, smartboards, where the child is playing or eating during break time and other appliances inside the daycare center. Smart daycares for childcare are made up of smart equipment and automated technologies. Everything is interconnected with the advent of the Internet. Simple daycare automation relies on timers and clocks to complete tasks, but smart daycares for childcare technology can handle more sophisticated tasks and activate devices based on inputs from other devices. In the Lambussie District, traditional open daycare system is practiced. The security of kids and teachers are at the mercy of God. The District is sharing

border with Burkina Faso where kidnappings and other militant operations are on the increase with high rate of kidnapping. In 2007, 4 kids were kidnapped to Burkina Faso while they were on break at winner's academy daycare school. It took several interventions to get these kids back home. The high rate of insecurity reduced enrollment of students and teachers' attendance which possess great concerns for parents and other stakeholders. In the global and local perspectives, some challenges of childcare implementation are irregular communication between teachers and parents, poor safety of kids in school, difficulty in tracking behavior, learning and developmental progress, too much paper work which is time consuming as well as security and privacy issues (Nivedha et al, 2020). To overcome these challenges, this thesis proposes and develops a secured IoT based smart daycare model/system to help ensure the security of its kids and promote effective teaching and learning.

1.3 Statement of the Problem

Security threats in Ghana have become a major challenge for both security personnel and residents in recent years. Kidnapping has been a very widespread problem in our culture in recent years. Contract killing has also made its way into the country seemingly out of nowhere. Kidnappings, deaths of children, adults, and the elderly are all over the news, with no one knowing how they happen. Day in day out, there are several reports of missing children, who are particularly susceptible to security threats when they go to and from school most especially kids in daycare. A total of 504 cases of kidnapping have been reported from 2011-2019, according to the Minister of Interior of Ghana, Hon. Ambrose Dery, in a recent address to Regional, Divisional and District Crime Officers at a two-day conference. Sulley (2019). This implies that

on the average, about 56 kidnapping cases were reported annually. In the Interior Minister's report, 47 cases had already been recorded for the year 2019. The cases of kidnapping and abductions are relatively dispersed across the various regions of Ghana including daycare children of which Lambussie District of the upper west region is no exception. Also, the daycare schools only operate manual system. As a result, there was the need to propose and develop a secure IOT based smart daycare system which will ensure that children are safe, secured and protected while at school, and also when being picked up from school. There will be checks to find out whether the child is indeed related to the person who is taking him or her out from school premises.

The user of the smart daycare system monitors and operate the security system using smoke detectors, CCT cameras and other smart devices. Teachers can also use the system to automate some school processes to enhance effective teaching and learning. Also, if attackers hack the smart daycare or a smart device, door locks are installed so that they cannot breach users' privacy, steal private information, as well as monitor the people within the building.

1.4 Research Objectives/Purpose of the Study

The purpose of the study was to propose and develop a conceptual model/system for the implementation of IOT based smart daycare center in Ghana.

The research objectives are:

1. To assess the extent of need/effectiveness of IOT based smart daycare system by teachers and parents in daycare schools in Lambussie District.

2. To identify potential security threats associated with IoT based smart daycare implementation in the Lambussie District.
3. To determine the effects of IOT based smart daycare system on the effectiveness of teaching and learning in Daycare schools in Lambussie District.

1.5 Research Questions

The following research questions were developed:

1. To what extent is the IOT based daycare system implementation needed by Teachers and parents in daycare schools in Lambussie District?
2. What are the potential security threats associated with IOT based smart daycare implementation in Lambussie District?
3. What are the effects of IOT based smart daycare system on the effectiveness of teaching and learning in daycare schools in Lambussie District?

1.6 Significance of the Study

The research findings will be useful in providing a better understanding of the extent of need/effectiveness of the system, the effects of the system on the effectiveness of teaching and learning and security threats related to the topic, as well as making people (users) aware of the potential risks and the measures that can be taken to mitigate these risks, either directly or indirectly, in relation to their Smart daycare for Childcare. Hopefully, the findings will inspire others to conduct more study in the issue of security in Internet of Things (IoT)-based Smart Childcare. This research will result in a list of proposed security dangers, as well as probable

repercussions, remedies, and suggestions to users in order to make them aware of the risks and reduce their exposure to them. It will also determine the extent of need / effectiveness of smart daycare system implementation in schools as well as determine how the IoT smart childcare system affects the efficacy of teaching and learning in daycare schools. Furthermore, the lessons acquired from the procedure in the instance of security risk assessment will help to improve future work. The findings of this thesis may be utilized to improve IoT technology deployments in Smart Daycare for Childcare in terms of security threats and its effectiveness in teaching and learning in Ghana.

1.7 Scope and Limitation

This study focused primarily on the extent of need/effectiveness of smart daycare system implementation, identified some security concerns (risks) and appropriate countermeasures and developed a security system for the smart daycare environment as well as assessed the smart daycare system deployment on the effectiveness of teaching and learning in daycare schools. Also, the study was limited to daycare schools in the Lambussie District of the Upper West of Ghana. The study also encountered some limitations, these are; inadequate resources and small sample size.

1.8 Organization of the study

This research is organized into five chapters, the first of which discusses the background of the study, statement of the problem as well as the purpose of the study. In addition, chapter two is devoted to literature review which examines what other publications, researchers, and authors

have stated and contributed to the topic the researcher is attempting to address. Furthermore, Chapter three delves into the methodology, data collection instrument, research design, and smart daycare architecture model/system in depth, while Chapter four examines and discusses the findings and the smart model system and Chapter five summarizes, concludes, and makes recommendations for future research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter explains various literatures and approaches in a secured based IoT smart daycare. The chapter is divided into four sections, section 2.1 gives the introduction to the chapter. Section 2.2 talks about conceptual framework. It explains the various concepts that are related to the topic. Section 2.3 explains the empirical framework. It reviews literature on other systems related to the topic. Finally, section 2.4 talks about the theoretical framework of the study. It also discusses the existing behavior prediction approaches in smart daycare automation.

2.2 Conceptual Framework

This involve Arguments regarding why the issue one wants to research is important and why the methods recommended to examine it are acceptable and rigorous (Riggan and Ravitch, 2017). It includes the concepts, assumptions, expectations, beliefs and literature that supports and inform the study. It explains the major object to be investigated that is; factors, ideas, or variables, and the hypothesized link between them, either visually or narratively.

The concepts in the topic are discussed below:

2.2.1 Internet of Things (IOT)

Kumar et al (2019) opined that IoT is a new paradigm that seeks to change the traditional way of living into high tech lifestyles. Several IoT applications are dominant in the market such as smart home, smart cities and so on, a survey conducted on global distribution of IoT applications reveals that industry, smart city, smart energy and smart vehicle based IOT projects have a big

market share in comparison to others. Smart city is one of the trending application areas of IoT that incorporates smart homes as well.

The Internet of Things (IoT) is a dynamic global network infrastructure comprising physical devices connected to the internet all over the world, all collecting and sharing data (Madakam, & Ramasmami, 2015). An IoT ecosystem, according to IOT agenda Tech group comprises of web-enabled smart devices that gather, send, and act on data they acquire from their surroundings using embedded systems such as CPUs, sensors, and communication hardware. By connecting to an IoT gateway or other edge device, IoT devices can share sensor data that is either routed to the cloud for analysis or examined locally. Smart daycare, smart cities, smart healthcare systems, intelligent traffic control lighting, linked vehicles, smart environment monitoring in industries, smart grids, smart metering, water network monitoring, smart logistics, and many more are examples of Internet of Things applications.

2.2.2 Smart Daycare Architecture model/system

This model encompasses the central management unit, user interface, home equipment and appliance interface, as well as external communication interface. It explains how the daycare management system works as well as the different sub-models that constitutes the system. The operating system, database, artificial intelligence engine, and application services are all part of the central management unit (Apthorpe et al, 2017).

Figure 1: Smart Daycare Model Architecture Diagram

Source: (Alheraish, 2014)

2.2.2.1 Central Management Unit (CMU)

The CMU is at the heart of smart daycare architecture, and all devices are connected to it by either wireless or wired connection. The CMU controls devices and equipment, manages preprogrammed scenarios, and communicates with external resources. CMU monitors, operate and control all smart-daycare components by checking status and sending commands. The CMU uses application software-services, equipment, and built-in database (local DB) information, stores preferences and operation modes. With artificial Intelligence (AI) components, the CMU can manage smart scenarios and emergency situations. The CMU's independent operating system bridges between smart daycare components and different interfaces, thus allowing for constant device control, and immediate response in case of errors, alarms or pre-programmed activity (Delgado et al, 2009).

2.2.2.2 User Interface

According to khiyal et al (2009), Smart daycare UI provides the user with access to some or all of the integrated devices and appliances in the home. Once the user selects a device, its current status may be displayed, as well as the menu of available commands. Equipment may be associated with a particular group of activities, such as lighting, entertainment, security, etc., location or any combination of group and location. Access to a specific device is subject to authorization and the UI's ability to control its functions. User Interface devices can be of various levels of sophistication, e.g., playing music or using the home entertainment system may be controlled by simple UIs, such as mobile phones or by more advanced interfaces, such as PDA (Personal Digital Assistant or pocket PC), touch screens, High-Definition Multimedia Interfaces, and others. Interfaces based on the mobile phone menu are useful for simple commands, requiring limited display. More advanced devices allow better use of graphics and software, and may present various screens.

Selective menus or options are based on UI device settings, stored in the CMU database.

Software application programming interfaces (APIs) are used for operating external applications, such as online shopping, whenever a smart refrigerator senses a low supply of groceries. APIs are facilitated to operate devices using their built-in functions, based on standard commands and communication protocols.

2.2.2.3 Indicators: khiyal et al (2009) opined that, besides the operating equipment, UIs display current state, ongoing activities, warning messages and relevant information. Based on the device's UI capabilities and the nature of the information, some of the messages/indications will automatically display, while others appear only upon request.

2.2.2.4 Programming and statistical data: Different forms of UI may be used for accessing the CMU. Direct CMU access allows system programming, adding new devices, displaying reports, charts, and statistics, i.e., equipment usage, errors, alarms and warnings. Equipment manufacturers may contribute by configuring UIs to access further information, such as help screens for complicated tasks, scenario programming, and consumption related information (Alheraish, 2014).

2.2.2.5 UI device specification: The proposed model provides different devices for smart daycare operation and control. Devices will differ according to size, mobility, supported communication protocols, displays and operation media, such as keyboard, touch screen, voice, and biometric sensors. The universal model defines smart daycare devices operation, using UIs compatible with mobile (or standard) phones, PDAs, personal computers, laptops, tablet-PCs, sensors, and biometric devices (Apthorpe et al, 2017).

2.2.2.6 User Authorization: Most of the smart daycare equipment may be used with no access restrictions. However, security systems or actions involved with potential risks such us heating or cooking operations, require user login; thus, user privileges settings are essential (Kasteren et al, 2009). In order to maintain proper access control, the following guidelines should be implemented:

- Any UI related to access-controlled tasks must include user login options.
- Any commands or properties defined as ‘access-controlled’ will be hidden prior to login.
- An active log-off time-out mechanism must be included in order to prevent misuse by non-authorized persons.

2.2.2.7 Home Equipment and Appliances Interface

According to Konidala et al, (2011), smart daycare equipment is currently being globally supplied by a wide range of producers and vendors, genuine integration of components and functions requires a set of standards and guidelines. At the same time, flexibility is necessary, in order to avoid malfunctions.

The following guidelines are important for enabling integrated smart daycare architecture:

A set of hierarchical commands, functions or accessible attributes for controlling and operating each integrated device. Each function or command may be independent, or a link in a chain. It should be predefined and recognized by the CMU.

The equipment manufacturer determines the interface's "look and feel". Yet, the user's access to each one of the supported controls/functions has to comply with at least one of the UI standards (lists, icons, scrolling selection list, 3D widget), in order to assure a generic model and compatible appliances. Different forms of equipment embody diverse functionality and purpose. Thus, the suggested model refers to commands and properties only, regardless of the intended uses, main features or specifications. Any other device must comply with at least one of the standard communication protocols.

Some of the integrated devices, mostly those associated with multimedia and security, require a flow of information, either one-way or bidirectional. In order to utilize the common home infrastructure, streaming-dependent devices must support popular formats, such as MP3, MPEG-4, WMA/V, Flash-Video, QuickTime, etc.

Programmable devices contain a built-in database for storage and data retrieval. In order to better utilize an integrated environment, it is strongly recommended to allow online CMU connectivity

(at least read-only) in order to provide online, continuous data exchange, and control of the local database.

Some equipment functionality and control examples as proposed by Konidala et al (2011) are as follows:

2.2.2.7.1 Security/environment control doors and windows: Doors and windows may be either opened, closed (unlocked) or locked. Open, Close, Lock and Unlock commands allow users to operate doors and windows, while Closed and Locked properties allow users to monitor current status. Each connected window or door may be accessed by either choosing a specific room or by its description (i.e., 'garage door'). Houses equipped with more advanced windows bring in new attributes, such as Shading Level, and Landscape Change, which may be monitored or modified.

2.2.2.7.2 Light control: Bulbs and light fixtures may be switched on and off. Additional properties, such as light color and intensity, may be controlled or monitored. In such cases, a command, such as Change Color, may require selection of one color/color scheme out of a given list. Light intensity, on the other hand, may be changed by using commands, such as Increase Light, Decrease Light, Set Light Amount or Max Light to a specific level.

2.2.2.7.3 Streaming devices: Multimedia devices or security cameras may be used as either a source or target for streaming data. These devices require a complex set of commands and properties. Some basic functions include: channel selection, format and compression, streaming direction (input, output or both), as well as movement and zooming options (zoom in, zoom out, rotate right, rotate left, tilt up, tilt down). In addition to the listed commands, a device's status is checked using attributes, such as: ready to transmit/receive, current format, auto focus enabled.

2.2.2.7.4 Smart appliances: Scenario-management allows users to define a set of behavior rules. For example, a smart refrigerator tracks inventory levels, and the expiry-date of stored groceries, thus assisting home residents with shopping and planning whether they are at home or away.

2.2.2.7.5 Voice, light and motion detection: Voice recognition applications and motion detectors may assist elderly people and persons with special needs. Motion detection equipment saves energy and essential resources by automatically adjusting climate control systems and lighting, based on current owner location, or estimated time of arrival to the house. Light sensors switch on outdoor and indoor lights at sunset, or control garden watering systems, according to the current weather conditions, sun radiation level, and humidity rate.

2.2.2.8 External Communication Interface

In order to allow maximum flexibility and optimal utilization of existing home communication infrastructures, the proposed smart daycare CMU is able to support various network standards and protocols, including Ethernet, X10 (electric wire-based networking), home PNA (phone lines), ZigBee, Infrared, Bluetooth, Wi-Fi, and others (Mokhtari et al, 2017).

CMU's application services and database store an up-to-date list of all connected and integrated devices. Any new integrated device is synchronized upon connection, and becomes inactive or is removed when not in use. This is done automatically by sending any shared data (list of properties, commands, optional streaming, etc.) into the CMU upon initial connection, and on predefined periodic processes. As put up by Mokhtari et al, (2017) Communication protocols and interfaces should support three levels of connectivity:

2.2.2.8.1 CMU control: Upon command initiation, the CMU sends either an action or inquiry call to a specific piece of equipment. The CMU then initiates calls in accordance with pre-programmed tasks or scenarios. A status checks or inquiry is conducted by sending a get command with the desired attribute to be checked. An action call involves set or any other supported command.

Unlike the get command, set or action commands require passing parameters. For example, the CMU may send a security system the following command: Arm (night mode). The CMU doesn't need to "understand" the nature of this command. Once the authorization level is satisfied, it sends the command and awaits a reply (if applicable). Such a command forces an action, rather than checks current status.

2.2.2.8.2 Device/Remote (external device) initiated call: Any built-in process or response may result in sending a call to the CMU. For example, integrated motion detection equipment will send a call to the CMU, following a particular type of behavior. When a motion sensor detects a movement in a particular zone, it sends the CMU a "message", resulting in a CMU response (dim lights, change climate setting, etc.).

Some calls may be ignored, depending on CMU setup and scenario management rules. Users may initiate a call from remote locations with their mobile phones or other communication device. For example, users may initiate a fill jacuzzi(95F) command to the CMU, which would in turn send a command to the hot tub, including the desired water temperature.

2.2.2.8.3 Streaming: Unlike single commands or inquiries, ‘streaming’ requires a continuous flow of data, for a defined period of time. The CMU stores extensive information about all streaming-enabled devices, including streaming direction, supported formats and compression.

2.2.2.9 CMU Components

The central management unit is further broken down into several components displayed by a pictorial view in figure 2. These components are

- Operating system
- Database
- AI (Artificial Intelligence) Engine
- Application service

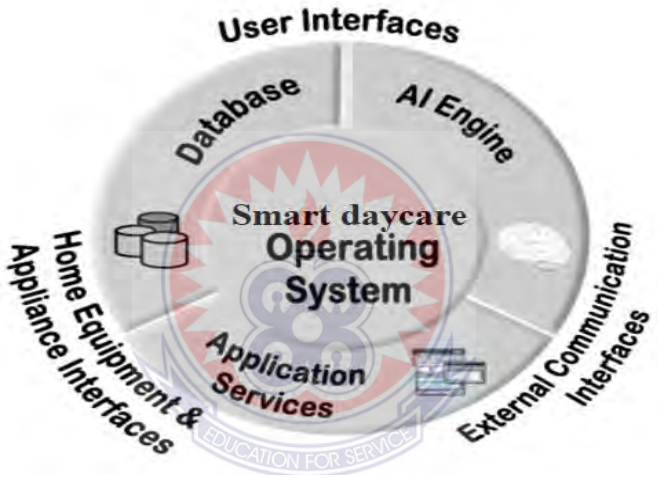


Figure 2: CMU Components

Source: Morsalin et al, (2016)

2.2.2.9.1 Operating System (SDCOS - Smart Daycare Operating System)

The CMU is responsible for continuous operation and control of all integrated smart daycare devices. It constantly monitors devices' status, sending and receiving commands and calls, recording events in the database, and so on. The SHOS identifies any compatible device, complying with the suggested standard, and orchestrates the entire smart environment.

2.2.2.9.2 The Smart Daycare Database

The database is the main storage point for all data in the smart daycare environment. Any connected device is registered upon connection. This process results in creating new records, describing all supported commands, functions and controls, communication options and other information. Connected devices (equipment and UI devices) have a built-in local database (LDB) which is used for storing current status, streaming data, scheduled tasks and a list of commands in the queue. The Smart daycare database is synchronized with the device's LDB, by sending and receiving commands and inquiry calls. The initial registration process loads all stored information into the CMU database from either a read-only chip or the LDB as shown in figure 3 3.

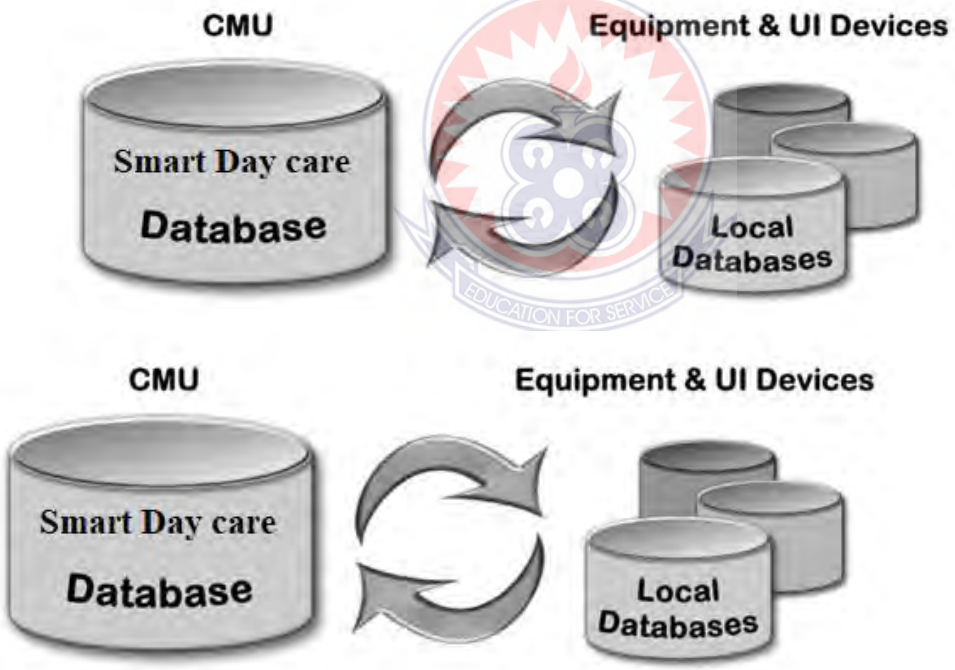


Figure 3: Smart Daycare Distributed Data- synchronization

Source: Saeed et al, (2010).

Table 2.1: Smart Daycare System List of Commands

Table	Description	Sample values
COMMAND	List of all device's commands	
COMMAND TYPE	Type of command	Check, assign, request-information
COMMUNICATION	Type of communication form	Input, output, both streaming
DEVICE	List of communication form	
DEVICE _COMMAND	Devices and commands relation	
DEVICE _TYPE	Device types	Security, climate control, entertainment, lighting
INTERFACE	List of available end user-interfaces	
INTERFACE_TYPE	Interface type	Character –based, GUI, Keyboard voice -activated
SCENARIO	List of programmed scenarios	
SCENARIO_ COMMAND	Scenario commands list and schedules	
SCENARIO_TYPE	Scenario type	Home entrance, away emergency, intra-home

Source: Apthorpe et al, (2017).

Table 2.2: Smart Daycare Database Data-Scheme

Table 2.2 illustrates a relational Smart Daycare-Database table scheme. Tables are either built-in or added upon installation of new devices.

Major database entities include:

Device	Any integrated component: lighting controller, door lock, appliance, sensor, etc.
Interface	User interfaces: phone, keyboard, touch screen, voice-activated device, PDA or others.
Command	Smart daycare devices inter-communication is handled by sending and receiving commands. A command may be used in order to check status, set attributes, activate/shut down a device or send information to another device/User interface.
Scenario	Set of pre-programmed, scheduled commands for devices operation, tasks initiation, or status checking.
Device	Any integrated component: lighting controller, door lock, appliance, sensor, etc.
Interface	User interfaces: phone, keyboard, touch screen, voice-activated device, PDA or others.
Command	Smart daycare devices inter-communication is handled by sending and receiving commands. A command may be used in order to check status, set attributes, activate/shut down a device or send information to another device/User interface.
Scenario	Set of pre-programmed, scheduled commands for devices operation, tasks initiation, or status checking.

Source: Saeed et al, (2010).

2.2.2.9.3 AI (Artificial Intelligence) Engine

According to Tapia et al, (2004), an important added-value of an integrated environment, versus a group of sophisticated appliances and devices, is the intelligent behavior of the smart daycare environment. The AI inference mechanism reacts according to changing conditions, reflecting suitable responses to different scenarios.

2.2.2.9.4 Application Services

The suggested smart daycare flexible architecture allows adding software models, in order to enhance devices operation and inter-device connectivity The Application Services model enhances the smart daycare by adding more flexibility in situations where commands or streaming data are insufficient for a materialization of a certain device. For example, programming a garden watering system may be much easier than using bundled software. The device manufacturer has to determine which of the supported UI devices is suitable to function as a medium for running the software, and develop compatible software accordingly (Sriskanthan et al, 2004).

2.2.2.10 Smart Daycare Situation Examples

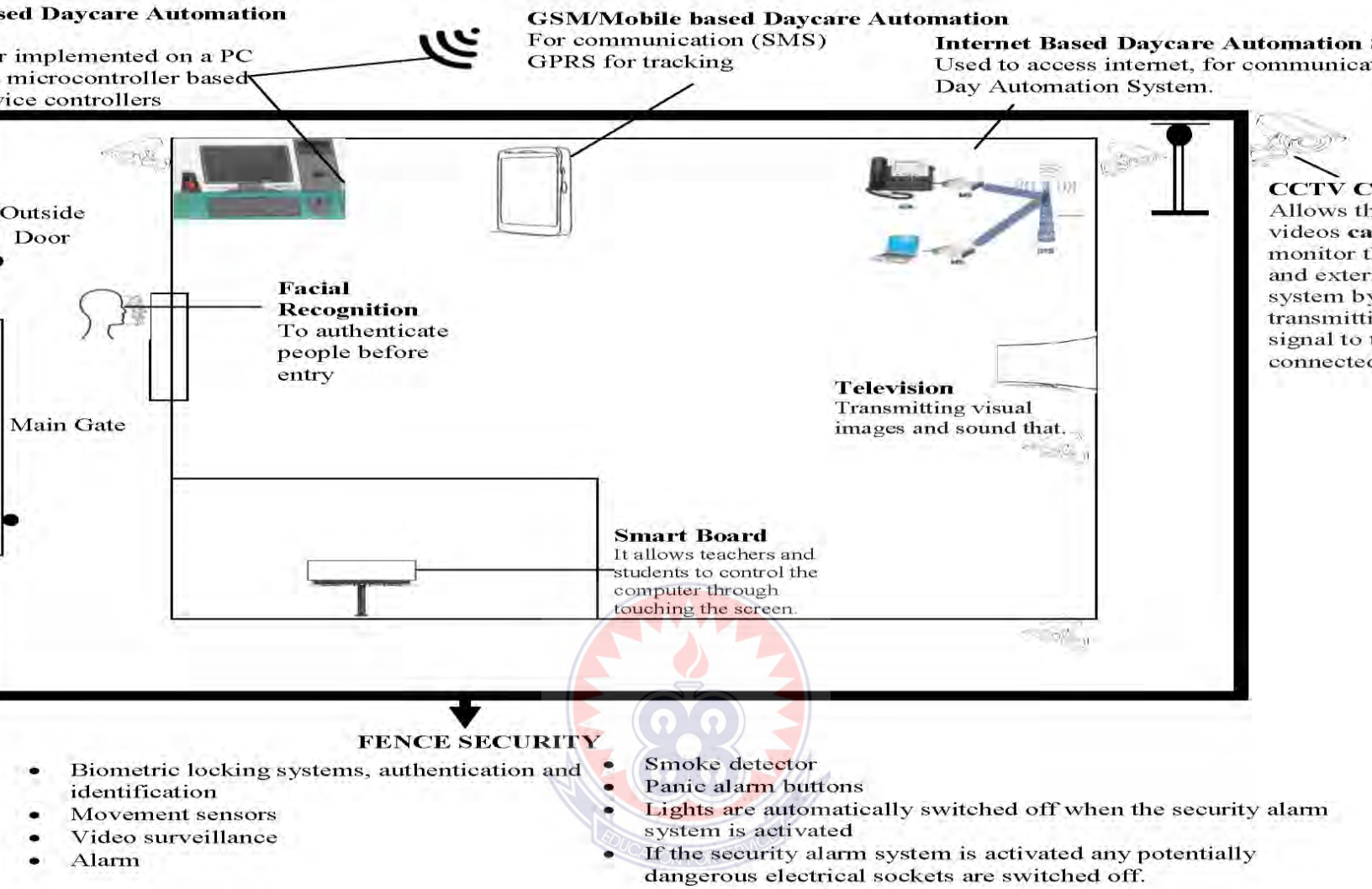
As proposed by Yang et al, (2016), the following examples illustrate handling common situations, following the smart daycare system's principles:

2.2.2.10.1 Daycare Cinema (Streaming Data): Broadband Internet connection and high-definition-supported devices enable new and exciting entertainment capabilities. Smart Daycare architecture makes it possible to watch streaming video on television screens, devices' monitors and projectors. Movies and other content, downloaded from the Internet or derived from Video-On-Demand (VOD) servers or any other resources, may be digitally recorded, thus assuring high quality viewing. For instance, a request to play a specific movie, on a certain monitor, at a desired time may be sent to the CMU. The CMU sends the appropriate request to the AI Engine, which in turn locates the best media source, either internal or external, and allows it to be stored temporarily or permanently, on any suitable content-storage device, such as hard-drives, optical

disks, and flash memory chips. Local stored content may be transferred to other devices, such as handheld computers, portable media players, television sets, etc.

2.2.2.10.2 Security: Protecting property when away from home. Comprehensive security systems combine wireless sensors, motion and sound detectors, indoor and outdoor surveillance cameras, and external communication. Once none of the residents are at home, devices and application services may monitor in-house activity in real-time, and use external communication interfaces or the Internet, in order to broadcast video, send alerts in case of emergencies, or operate defense systems. Calls can also be automatically initiated to the fire department or the police/security call-center. Smart daycare flexibility and APIs (Application Program Interfaces) allow different uses for specific devices. For example, a security indoor camcorder could also be used in order to monitor infants, displaying the video at home or at a remote location.

2.2.2.10.3 Special Needs: Various technologies can monitor the health of each child. Today, these technologies are currently being used. For example, people who suffer from heart disease transmit their ECG results over the phone. A smart daycare could also use more sophisticated AI technologies, monitoring children health indicators, and generating an alert when an unusual pattern is detected. The system senses a heart failure in real-time, and contacts the physician fed to the system directly. A smart toilet could perform routine diagnostic examinations, and save the results in a central database, accessible to the daycare physician. In the case of workers or staff at the daycare the system can learn to identify each person's typical behavior, and issue an alert whenever the common pattern of behavior is broken.



FENCE SECURITY

- Biometric locking systems, authentication and identification
- Movement sensors
- Video surveillance
- Alarm
- Smoke detector
- Panic alarm buttons
- Lights are automatically switched off when the security alarm system is activated
- If the security alarm system is activated any potentially dangerous electrical sockets are switched off.

Figure 4: Smart Daycare and its Subsystems

Source: Zheng et al, (2008)

2.2.3 Smart Daycare Environment

A daycare environment is a setting where students and staff come together to follow instructions while adhering to certain norms and regulations. To develop a safe internet of things, smart daycare environments use technological instruments (hardware) such as computers, phones, tablets, and other smart gadgets as well as controller systems to ensure the security of students and staff (IOT).

2.2.4 Model

A model is a representation of key concepts that is either pictorial or graphical. It depicts the connections between different sorts of variables (dependent and independent). A model is a method for approaching an issue. It's a more abstracted manner of schematizing a process, allowing you to apply your strategy to similar challenges in other domains. (Creswell & Plano, 2011). Tlaitlai et al (2021) proposed the green design model for daycare centers in Lesotho. Utilizing non-toxic play toys, usually made of organic materials like wood, is a component of green design. Toys should be non-toxic, vibrant, made of easily accessible materials such as cloth and with other natural components. The Department of Education and Early Childhood Development highlights the features that encourage children to explore and interact with nature include offering abundance of natural resources, healthy atmosphere and a place where technology is welcome. Findings indicated that children's safety, physical growth and mental development will be improved by the use of non-toxic building materials, appropriate ventilation designs, and smart automation systems in school.

2.3 Empirical Framework

This focuses on other writers' study, which looks at a variety of systems relevant to this topic such as surveys and scientific experiments. It is based on observation, experience and understanding of other works. It examines prior research and by criticizing it, demonstrates the research gap, as well as pointing to a new future direction that this model/system aims to clarify.

2.3.1 Context Aware Smart Daycare Automation Systems

Residents of a modern smart daycare can access it from the outside using internet/GSM and wireless portable devices such as phones, tablets, and laptops, as well as stationary equipment such as an office workstation (PC). Understanding the context of a user's behavior could go a long way toward enhancing home security.

Context, according to Dey (2001), is "any information that may be utilized to characterize the situation of an entity, where the entity can be a person, place, or item that is regarded significant to the interaction between a user and an application. In a context aware Daycare Automation System, the researcher is made to be aware of the context in which a user makes a decision and predicting the location of the user.

Schlitz et al. (1994) examine various ways for determining a user's location. The study suggests the use of an infrared grid to properly forecast the user's position, resulting in increased security. However, this grid of infrared sensors is difficult to deploy in a daycare setting. The work also examines the usage of badges to identify the location of residents inside the daycare, while this might considerably increase security, it is difficult for the user. Also, residents may be negligent in their current location and misplace these badges, causing system confusion. ‘Static Object

Checking' is another method outlined in the work. It determines an inhabitant's location by determining whether or not they are in the vicinity of static objects. This method limits the environment's adaptability, and if someone moves or alters the position of these static objects, the system will get quite confused.

According to Bellotti & Edwards (2001), Contextual sensing is also a challenge.

Human behavior is difficult to predict, individuals are unpredictable and unreasonable at times, in contrast to computers, which make instinctive judgements about their surroundings and improvise. Context aware computing creates severe privacy concerns for users. The system now has even more detailed knowledge about the user with context aware computing. In order to achieve context aware computing, the system will need to communicate this knowledge, which raises problems about who will have access to it, who has access to the shared information and how the shared information is used. In other words, the technology creates more privacy issues than it addresses. According to Intille (2002) stipulates that, the home of the future will not govern the environment but rather will assist its residents in learning how to regulate it on their own. In other words, robbing people of their ability to make decisions (as context aware computing does) will have a severe influence on their psychological health. Intille (2002) concludes that, instead of the system making a context aware decision on its own, smart daycare technologies should aid center residents in making energy saving or security conscious decisions by informing or reminding them when such opportunities arise in order for context aware systems to be successful in a smart daycare setting, the system must reveal what it knows to the user. What it knows about it and what it plans to do about it When a user's context-based activity has an impact on others, the System must alert them. Context Aware Computing significantly

increases the complexity of a system. It's difficult enough to accurately interpret the environment without the added burden of guessing the user's context (intention and reasoning for an action). Contextual computing raises the manufacturing, implementation, and maintenance expenses of a system, making it unaffordable to the average person. The system's success depends on continual user interference which most users find it irritating. Furthermore, only an expert or skilled individual can repair the system if it malfunctions. On paper, the concept of "context aware" systems is appealing, but it is difficult to execute correctly and raises major privacy concerns.

2.3.2 Central Controller-based Daycare Security System

A smart daycare security system based on a Central Controller aims to improve the security of homes in a neighborhood by merging many daycares to establish a security network with a control node devoted to each area based on the number of users. A few Central or Chief Control nodes with a lot of processing power are in charge of these control nodes. A central controller-based technique is used in the Daycare Security System on Intelligent Network (DSSIN). Modern security parameters are missing from the proposed system. The security solution based on a central controller has its drawbacks. All or most Daycares in the neighborhood have to join in for the approach to be cost effective and successful (Jose & Vigyakshmi, 2018).

Who controls or has access to the central controller and its data is the most important point to examine here. From the data at its disposal, the Central controller will be able to learn about a daycare's sensitive and private information, such as if a daycare's room heater is ON or if an occupant in a daycare is having a shower, etc., which creates major privacy concerns. We

already know how the public feels about government internet surveillance. The use of Central Controller-based security systems allows for even more intrusive surveillance of people's homes. Using GPRS, Atukorala et al. (2009) offers the 'SmartEye' Daycare Automation Security System. A central controller is also used by 'SmartEye to which numerous individual daycare controllers are attached. A real-time Daycare Automation and Monitoring System is proposed by the system. The technology sends a GPRS alert to the user's phone, and the user may monitor the daycare via live video feeds. To link an electrical equipment in the daycare to the daycare system, the system employs the 'RabbitCore' Model (usually a PC).

A central server is connected to each daycare system. 'RabbitCore' has an IP address so each device connected to it can be identified and operated via mobile phones using GPRS. The user transmits device management commands to the central server; the home system reads the command from the central server (a process known as "home polling") and makes the necessary adjustments to the device. When a device's status changes, the user's home system (typically a PC) broadcasts the change to the central server, which the user's mobile will read (a process known as "mobile polling"). The home design and locations where each piece of equipment is maintained in the home are presented to the mobile user.

The proposed study prioritizes communication and network setup over security; it mentions intrusion detection but does not provide actual parameters for detecting intrusions. 'SmartEye' is a security system that uses video cameras. Its security difficulties are detailed below. Furthermore, like many centralized daycare security systems, the proposed system is not designed to secure a single daycare but rather a collection of them, and the author's assertion that

"increased poll rate leads to increased security" is dubious and deceptive. In practice, a security system based on a central controller is difficult to install and creates major privacy concerns.

2.3.3 Bluetooth Based Daycare Automation System

Sriskanthan et al. (2002) demonstrate the use of Bluetooth to create a Daycare Automation System. They employ a PC-based Host Controller that is linked to microcontroller-based sensor and device controllers. The researchers even created a new protocol called Daycare Automation Protocol (DAP) on top of the Bluetooth software stack to allow devices to communicate with one another. The I2C Bus connects the device controller to the electrical equipment. This technology allows the Host Controller to be linked to several device controllers.

Kanma et al. (2003) also proposes a Bluetooth-based Daycare Automation System that can be accessed remotely via the General Packet Radio Service (GPRS). As a Host Controller (all home gadgets interact with this phone through Bluetooth), the researchers utilize a cell phone with Bluetooth connection and the Global System for Mobile Computing (GSM). Modem (modem) (provides internet connectivity).

Bluetooth communication adapters are installed in home gadgets so that they can connect with the Host Controller phone through Bluetooth. The research explains how to operate and update home equipment remotely, as well as how to diagnose and identify faults. The work also deals with providing an electronic user manual on the phone using Bluetooth and internet.

2.3.3.1 Issues of Using Bluetooth for Daycare Automation:

- Bluetooth has a restricted range of communication (maximum range of 100m in ideal conditions) that is required in a home environment.
- Because Bluetooth connectivity consumes a lot of power, devices' batteries must be recharged or changed regularly.
- Bluetooth technology has progressed and improved to Bluetooth Low Energy (BTLE), which gives the same range of communication (100m in ideal conditions), but it has severe security problems, such as eavesdropping and cracking encryption as highlighted by Ryan (1995).
- Bluetooth connection should only be utilized when a fast, short-lived network link is required with minimal regard for security.
- Bluetooth appears to be an appealing communication technology for implementing smart daycares; it is inexpensive, simple, and quick to set up, people are already familiar with the technology, the hardware needed to establish Bluetooth communication is readily available, also the technology provides the necessary bandwidth for operation in homes. However, they also have serious faults, as mentioned previously.

2.3.4 GSM or Mobile based Daycare Automation System

Researchers are interested in mobile-based Daycare Automation because of the widespread usage of mobile phones and GSM technologies. We primarily consider SMS (Short Messaging Service) based Daycare Automation, GPRS based Daycare Automation, and DTMF (Dual Tone

Multi Frequency) based Daycare Automation as GSM communication alternatives. The shortcomings of each of these three technologies are described below.

Alheraish (2004) advocated the interaction with home sensors, electrical, and mechanical equipment using a GSM model and a SIM (Subscriber Identity Model). The system uses a transducer to translate machine operations into electrical signals, which are then sent to the microcontroller. A transducer translates physical quantities such as sound, temperature, humidity, and so on into a different quantity such as voltage; in this case, the function is performed by a sensor. The readings from electronic equipment are sent directly into the microcontroller. The microcontroller decodes these signals and transforms them into commands that the GSM model can understand. Based on the received commands GSM model selects the appropriate communication method (SMS, GPRS or DTMF).

2.3.5 SMS (Short Messaging Service) Based Daycare Automation System

Alheraish (2004) offers an SMS-based smart daycare automation system. The suggested system detects unauthorized entry into the daycare and allows legitimate users to alter the door's passkey and regulate the daycare's lighting. The unlawful entry into the home is detected by utilizing LED (Light Emitting Diode) and IR (Infrared) sensors to monitor the condition of the front home door. The door's passkey can be any four numbers, which can be entered via the keypad or by SMS from a registered user's phone number. A user may manage the lights in their daycare remotely via SMS from their registered cellphone numbers, by turning the lights on in different rooms at random intervals of time, the daycare can appear to be populated even when it is not.

Khiyal et al. (2009) proposed the 'SMS Based Wireless Daycare Appliance Control System, a subsidiary of an SMS-based Daycare Security System (DACS). A daycare owner may manage their business by sending SMS messages to a pre-registered cellphone number. The system rejects SMS messages that are not sent from a valid user mobile number. In the event of an intrusion, the proposed system's appliance control and security subsystems send back an SMS to the owner.

An SMS-based Daycare Automation System is proposed by Saeed et al (2010). The system has a Java application running on the phone, and valid users may log in with their username and password and choose the building / floor / room, or device that they want to manage remotely, as well as a suitable action from the list of user actions. The Java program will construct and send the necessary SMS message to the GSM modem at home. The SMS message is received by the GSM modem, which decodes it and sends it to the home network for the requested action. For security, the researchers employ a 4-digit passkey and face recognition.

Delgado et al. (2009) employed GPRS connectivity as a backup for an internet-based Daycare Automation System, increasing the system's fault tolerance. The house owner will be able to receive warnings on their phone when the sensors' states change unexpectedly. The consumer might then respond through text message (SMS) or a web interface (internet). In any case, there will be two methods to get inside the home, so if one fails, the user will be able to fall back on the other.

2.3.5.1 Security concerns in SMS Based Home Security Systems:

Alheraish (2004) and Saeed et al (2010) utilized a 4-digit security passkey, which in itself suggests a security vulnerability. We can't expect the owner to be cautious every time he or

she inputs the passkey; an attacker might wait outside the daycare and look through the window to learn the passkey. This is because the user punches in, the passkey on a regular basis, the chances of the user becoming careless are great.

The passkey utilized by Saeed et al. (2011) is unique for each person at the daycare, increasing the chances of hacking the keypad. Furthermore, people who are prone to 'Social Engineering' and other attacks choose these passkeys. The majority of the recommended methods either ignore sophisticated attackers or are ineffective against them. Apart from the main entrance, the systems do not consider any other access points in the building. A skilled attacker could easily spoof the LED and IR sensors employed by Alheraish (2010) to detect intrusions.

Notifying the homeowner of a home intrusion by SMS is never a smart idea; users may not check their phones for SMS messages on a regular basis, or may not be close enough to hear the "message received tone," and so may miss the intrusion alarm.

Because the system can't tell the difference between an image and a real person, simple Facial Recognition systems might be hacked with a snapshot of an authorized person. Attackers are becoming increasingly clever in today's society.

Always keep in mind the potential of an attacker cloning the SIM card of a genuine device and doing all of the operations that a legitimate user undertakes. Furthermore, we can never rule out the chance of the user misplacing or the attacker stealing his or her registered mobile phone. If this occurs, "breaking into a home may be as simple as stealing a cell phone."

According to the researchers Delgado et al. (2009), remote access improves home security since the user may be notified of an intrusion as soon as it occurs and see the home through numerous cameras installed throughout the home. The research entirely overlooks the numerous security

vulnerabilities that exist in the gadgets that link and automate a home. Furthermore, when the home is linked to the internet, the chances of an attacker exploiting these vulnerabilities grow dramatically. Furthermore, the cameras utilized in this research have security challenges, which will be explained further down.

2.3.6 GPRS (General Packet Radio Service) Based Daycare Automation System

GPRS is used in a large number of daycare security systems. Most systems employ the term "security" in the traditional sense, addressing solely the threat posed by old fashioned intruders. The researchers Danaher and Nguyen (2002) suggest a GPRS-based home security system. The system employs a camera to send video and photos of the home to the owner's phone through GPRS. By comparing frames for changes, including light intensity, the webcam identifies movement. The suggested approach uses a home internet connection rather than a GSM modem to broadcast video.

Wu et al (2006) present a video camera (that can also take still photos) surveillance system that uses the GPRS feature of mobile phones. When an intrusion is detected or the doorbell rings, the camera is activated. An infrared sensor in the system detects intruders. When the doorbell rings, the system notifies the homeowner and initiates voice conversation (along with the live video stream) between the visitor and the homeowner. When an intrusion is discovered, the user receives an email containing a photograph of the invader. The user then begins viewing the video feed on his phone as soon as he receives this email.

Using GPRS at the daycare facility, Yang et al. (2006) allows a user to read and alter the state of the devices using a preregistered mobile phone. External devices cannot link directly to the

devices in the proposed system. When a genuine device (recognized device phone number) attempts to connect to the daycare environment, a link is created between the virtual daycare (which functions as a honey-pot) and the user. The commands issued by the user are analyzed, and if they do not endanger the daycare devices, they are applied to the actual devices. When an emergency situation arises (intrusion is detected or Fire outbreak) the intelligent devices at the daycare initiates a communication between the daycare and the user (via telephone, text message, email) called 'phone-out-only' (Not the other way around i.e. user never initiates direct communication to home devices).

Another home and office automation system employing GPRS in mobile phones was proposed by Ali et al. (2006). A client/server architecture built at home utilizing a PC and a tiny Java application allows the user to communicate with the home. A device controller linked to the PC's parallel port is used to control home gadgets. Users can remotely operate and inquire about the status of devices linked to the device controller using the suggested system. A Daycare Automation System based on Wireless Sensor Networks (WSN) and GPRS was also discussed by Jin et al. (2008). It lets customers to utilize their mobile devices to operate equipment in their homes, collect data on device status, and monitor weather conditions at home. Users get information about house invasions and fires via Chinese Instant Message Mobile Service, which the authors customized for China. Unlike existing GPRS-based Daycare Automation systems, the proposed system employs a central controller based on an embedded system.

Das et al. (2011) used GPRS to create an iOS-based Daycare Automation Security System. For communication, the suggested system employs a client/server model. The authors create an iOS app that runs on users' phones and functions as the client while the cloud to which the home

devices are linked, serves as the server. For home security, the researcher employs video cameras, microphones, and motion sensors. When a motion sensor is triggered, video cameras in the locality begins recording; users can view live feeds on their mobile devices through GPRS. A web browser can also be used to access the proposed system.

2.3.6.1 Security concerns in GPRS Based Home Security Systems

Das et al. (2011), Dana heb & Nguyen (2012), Wu et al. & Yang et al. (2006), implements cameras at home. Streaming live video feeds over the internet is never a smart idea, especially when it is coming from within the home; if the cameras are compromised, the attacker will get a look inside the home. Wireless cameras are vulnerable, according to a recent BBC investigation by Kelion (2014). Furthermore, individuals dislike being shriveled since it disrupts their regular behavior and makes them feel uncomfortable.

If the cameras and the system are not setup and maintained properly, sophisticated attackers may be able to loop video feeds. To successfully fight against invasions in a GPRS-based intrusion detection system, the user must continually check his or her phone. Wu et al. (2006) effectively uses IR sensor-based intrusion detection system to identify and question intruders since it can be faked by a competent attacker. Yang et al. (2006) utilizes words like "safe", "do not harm" that have a broader meaning and are not defined explicitly. Furthermore, experienced attackers might impersonate real user mobile numbers in their proposed system, allowing them to influence or at least know the state of home devices; given the status of different home devices, one can deduce whether a home is occupied and which rooms are occupied.

Notifying a user of an intrusion attempt through email is never a smart idea; consumers may not check their phones for email messages on a regular basis or may not be close enough to hear the "message received tone," making the intrusion notice easy to miss. Researchers Das et al. (2011) provides consumer access to their homes via a web browser, which exposes them to a variety of browsing-related security concerns such as session hijacking, cookie theft, Cross-Site Scripting, and so on. Danaher and Nguyen (2012) provide only basic security because they rely solely on cameras and no additional security controls. To identify intruders in a home setting, almost all GPRS-based Home Security Systems employ one or more of these devices, such as video cameras, motion sensors, or infrared sensors. To detect a more technically proficient attacker, they rarely utilize any complex procedures or algorithms.

2.3.7 Internet Based Daycare Automation System

In the Daycare Automation System, Internet or IP protocol-based communication is always a popular choice among researchers. The Internet is easily scalable, flexible in terms of access and use, and very popular as a communication method in today's world, so the hardware and network required for access are readily available. It also provides high bandwidth at a low cost of communication, and devices can easily connect and disconnect from the network. These are some of the characteristics that make the internet such an appealing option for researchers.

The use of the internet to access and operate homes appear to be the next logical step in the development of Daycare Automation Systems. From the perspective of the end user, using the internet to access their home is simple, convenient, inexpensive, and flexible; there is no additional technology to learn, and user interface devices such as laptops, smartphones, PCs,

tablets, and other similar devices are readily available in the market and are already a part of people's daily lives. As a result, integrating Daycare Automation into these already popular consumer gadgets appears to be a logical next step. The components of a typical Daycare Automation System using the internet is depicted in the diagram below:

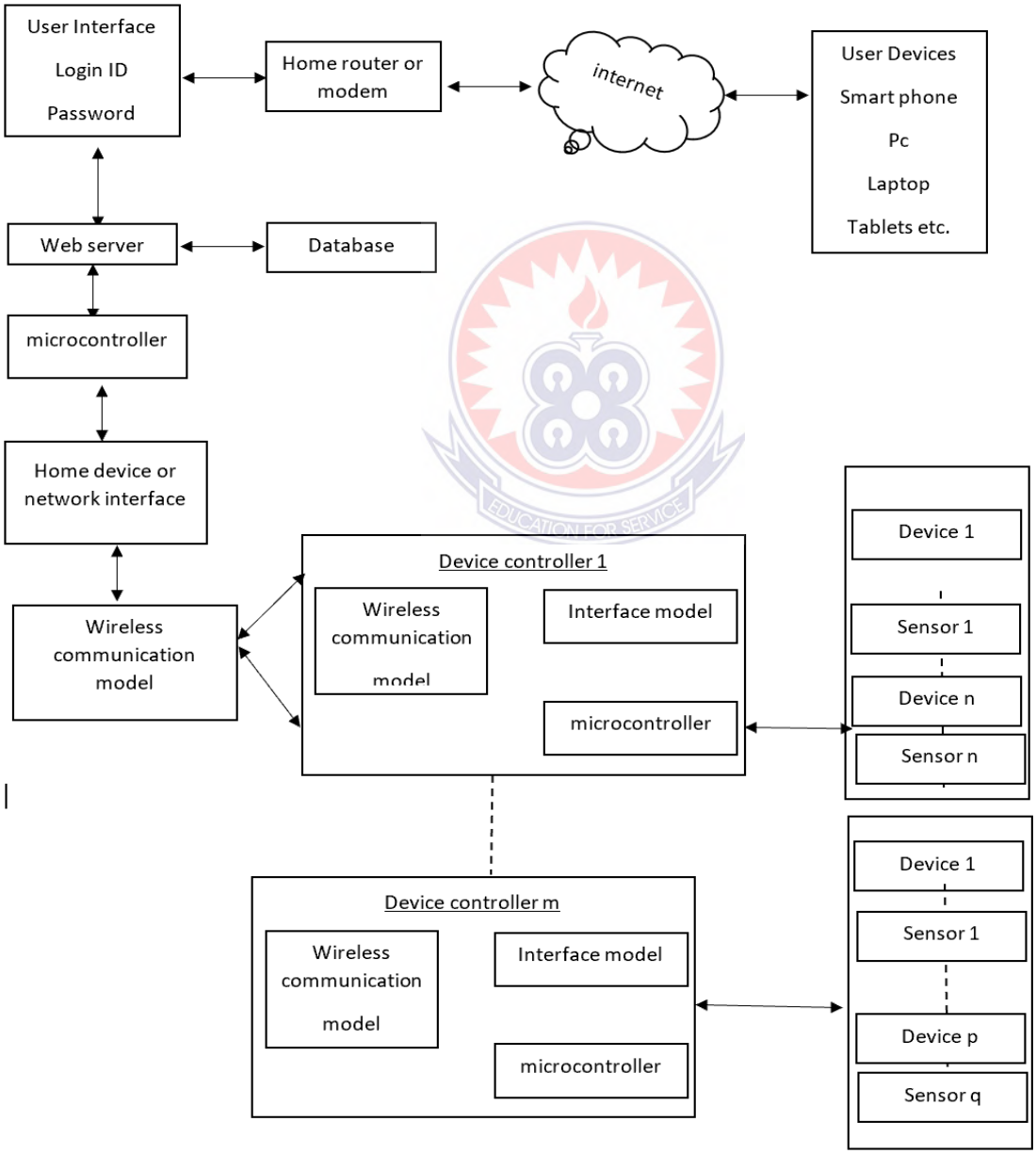


Figure 5: Logical Diagram of a typical Internet based Daycare Automation System

The User Interface (UI): User Interfaces are generally web pages or any Android, iOS, or Windows applications that the researcher has created. A user can use these programs or web browsers to connect to their home through the internet from their mobile devices. Before providing entry to the home, most Daycare Automation Systems employ a "username" and "password" to identify genuine users. Most Internet-based Daycare Automation Systems appear to employ simply username and password authentication, which poses certain security concerns: People are inherently irresponsible, and they frequently scribble difficult passwords and usernames on paper near their workstations or beneath their keyboards, thinking 'who bothers to look there'.

People frequently use the same passwords and identities across many websites and forums, making them vulnerable to phishing attacks. A homeowner will have to login to their home from various networks over time, such as the workplace, a friend's house, and public Wi-Fi networks such as coffee shops, parks, and so on, occasionally using untrusted devices. The user's network of choice for accessing the home may be vulnerable, exposing the user to threats such as a "Man-in-the-Middle" attack. Furthermore, by using simple software tools like ‘Keylogger,' valid user credentials might be stolen while entering the home from a compromised device. When relying solely on passwords for security, researchers should be cognizant of the ‘Human factor.' The ‘human factor' refers to the fact that most individuals select passwords that are meaningful to them, such as the names of their pets, favorite movies, musicians, sports teams, and so on. Furthermore, we must never overlook the most potent of all hacks, ‘Social Engineering,' which

may be highly efficient when attempting to get a person's password and login. When a home is accessed through a web browser, it becomes vulnerable to the browser-related security problems described previously. When it comes to accessing their home through the internet, researchers must anticipate that if given the option, individuals would pick convenience above security. The Microcontroller, the Web Server, and the Database: A web server connects the user interface to the database. The database contains information about all of the home devices as well as their current condition. A user with remote access to their home can use the web server to query the database for device status information. A Microcontroller manages all the operations and communications in the home network. Because a PC can do all of these functions in reality, researchers have chosen to replace these three components (web server, database, and microcontroller) with a PC for ease of use. Network interface model: It coordinates communication between the PC and the controllers for home devices. When a user gives orders to modify the status of the gadgets in the home, the commands are sent to the device controllers via this interface. The status of a device is sent to the database through the interface once these commands are completed. Device Controller: A Device Controller comprises of an interface model, a wireless communication model, and a microcontroller to control its operations. Multiple home gadgets and sensors are linked to a Device controller. The device controller relays user orders and status inquiries to a home device.

2.4 Theoretical Framework

Theoretical framework is used in conjunction with the conceptual framework to explain the relationships investigated in the study, (Ravitch & Riggan, 2017). It places the relationships

investigated in the study in the framework of formal theory development or testing. The research also discusses various relevant ideas, methods, and models, as well as the relationship between smart daycare architecture, smart daycare environments, and the internet of things. The system management theory and the social system approach/model are two examples of theories connected to childcare or human management. It also reviews literature on device fingerprinting and logical sensing approaches to smart daycare.

2.4.1 Device Fingerprinting

This section discusses the existing literatures related to device fingerprinting. Various methodologies, parameters, and strategies for detecting and obtaining device fingerprinting parameters are also discussed in this section. The term "cookie" was first used in the context of a web browser (Loutenon, 1994). Cookie technology allows webservers to store a small amount of data on the computer of a visiting user, which is then transmitted back to the server when the user requests it. Browser manufacturers rapidly adopted the concept of cookies. As a result of the cookie's state-full design, attackers began to take advantage of it soon after. Cookies were utilized by third-party advertising sites to monitor visitors across various websites, which encouraged behavioral advertising. This privacy-invading behavior drew the attention of the research community, the legal community, and the general public. Cross-Site Scripting and Cookie Stealing are also threat to cookies. The term "cookie" was broadened to include Flash cookies and, subsequently, the term "evercookie," which is nearly difficult to delete. The privacy concerns about cookies were heightened as a result of this. One in three users erased their first and third-party cookies after a month of visiting a website, according to cookie retention

research. The aforementioned studies demonstrate the privacy, security, and unavailability concerns that come with identifying a user via cookies. As a result, using cookies in Daycare Automation to identify a user via the internet does not appear to be a good idea.

Because of the problems with cookies, academics and online advertisers devised a new method of tracking internet users. Mayer (2009) and Eckersley (2010) demonstrated how the characteristics of a web browser may be utilized to uniquely identify a person over the internet without the usage of cookies. Mayer (2009) conducted research on 1328 web clients. He hashed the combined contents of navigator, screen, navigator, and mime Types in his study. Mowery and Shacham (2012) presented a device fingerprinting method based on the assumption that various browsers render text and images differently. This disparity arises from a mix of software, browser, driver, hardware, and GPU configuration variations. The researcher made use of this by rendering text and Web Graphics Library (WebGL) scenes into an HTML 5 canvas> element and measuring the difference in the pixel map of the canvas for various users. The suggested approach is unable to distinguish between two web clients with identical software and hardware specifications, and it will not function with earlier web browser versions.

Device fingerprinting via clock skew was proposed by Kohno et al. (2005). The authors discovered that any two physical devices have a distinct clock skew difference, and that this unique clock skew difference between two devices would stay reasonably stable over time. They made use of this clock skew capability to fingerprint a remote physical device by secretly recording and analyzing its ICMP or TCP timestamps. The use of ICMP and TCP timestamps have its drawbacks. ICMP timestamps are prohibited by many firewalls, and some operating systems deactivate TCP timestamps by default. Later, Zander & Murdoch (2008) devised a

synchronized sampling device identification approach that greatly decreases quantization error. It decreases the amount of network traffic required for prior identifications, and their work was the first to use the Hyper Text Transfer Protocol (HTTP) protocol to compute clock skew estimate. However, their method for device identification could not be directly applied at the server level. Huang et al. (2012) were inspired by this work and created a client device identification in a cloud computing environment that uses JavaScript to transmit periodic timestamps back to the server for device fingerprinting. Nakibly et al. (2015) developed a device fingerprinting approach that makes use of the uniqueness of hardware features such as speakers/microphones, motion sensors, GPS accuracy, battery charge and discharge duration, and GPU clock skew. For the time being, the majority of their recommended approaches are simply theoretical. Furthermore, their fingerprinting method necessitates continual user engagement, which is not ideal.

2.4.2 Logical Sensing

This section narrates various literatures associated with logical sensing and their shortcomings. To anticipate and learn user context, Choi et al. (2005) used body temperature, pulse, facial expression, room temperature, time, and location. Their research ignored the fact that a user's body temperature, pulse, or facial expression might change depending on a variety of other circumstances such as their mood, sickness, and so on. Furthermore, their work employs the usage of cameras to interpret facial expressions, which, when hacked by a tech-savvy attacker, introduces additional security and privacy concerns into the home.

Context aware sensing, according to Yurur et al. (2014), changes based on the user's surroundings, prior knowledge of current event patterns, user perception, and context. It is

exceedingly difficult to predict the context of diverse user behaviors in a home environment because individuals are relaxed, spontaneous, and unpredictable. This makes context aware computing difficult to execute unless the system has a thorough understanding of the situation, which necessitates advanced sensing techniques and a lot of processing capacity. Context aware sensing is an expensive proposition for smart daycares due to advanced sensor techniques and high processing power. Furthermore, during context aware computing, the system deals with extremely personal and private information about a user and his behaviors, which must be given in order for the idea to work, which creates severe privacy concerns.

Saponara (2012) illustrated how an attacker may use power usage to detect which gadgets are operating in a home at any given moment. As a result, implementing a totally context-based security system in a smart daycare is dangerous and costly. As a result, this thesis focuses on user behavior at multiple access points rather than the context in which the user makes a decision.

According to Konidala et al. (2011), radio frequency identification (RFID) tags can be used to successfully identify various objects within a smart refrigerator. This approach might be applied to increase house security, but it necessitates the use of RFID tags on most things within the home, including the residents, which is unpleasant and difficult to execute given human's nature and tendency for forgetfulness. Lee et al. (2004) employed an infrared (IR) grid to locate inhabitants in a smart daycare.

Multiple infrared sensors were installed on the ceiling to create an IR grid that could predict occupant location inside a residence. Later, Kim et al. (suggested using a Bayesian classifier to enhance projected occupant location accuracy inside the home. Kumar & Kumar used an

Arduino Uno microcontroller and an IR motion sensor to detect infiltration attempts in a home, and when one occurs, the information is sent to the user through GPRS to their Personal Digital Assistant (PDA).

In the suggested method/model proposed, the users have to be near their phone in order to be notified of an intrusion attempt. Furthermore, competent attackers might fake the researchers' infrared sensors. For intrusion detection, this thesis uses ultrasonic proximity sensors, force sensors, contact sensors, and gas sensors in addition to IR motion sensors. Zhao et al. (2005) suggested a low-cost, adaptable home security system that sends an SMS to the administrator in the event of an intruder. To detect attack attempts, their method lacks advanced intrusion detection techniques.

Morsalin et al. (2016) proposed a home security system that included a Near Field Communication (NFC) tag, passwords, and fingerprint recognition. The system also has an embedded Global System for Mobile (GSM) model that uses Machine to Machine (M2M) connection to send the recorded password to a distant server. It is inconvenient for a user to have to enter his password and verify his fingerprints every time he wants to access his home. A careless user could lose the NFC tag mentioned in the paper, or an attacker could steal it.

Huang et al. (2016) developed a video-based fire detection and identification approach, which is too costly to be employed in a smart daycare setting. It also necessitates the installation of video cameras within the home, which, if hacked, poses a severe danger to the privacy of the residents. The thesis's fire detection system uses temperature and humidity sensors, as well as gas sensors, to detect fire.

2.4.3 Behaviour Prediction

This section details various approaches to behaviour prediction in smart daycares, most of the literatures here are focused on improving the efficiency of the smart daycare rather than focusing on security.

Over time, several user identification techniques have been proposed, ranging from basic passwords, fingerprint verification, retinal scan verification, face recognition utilizing cameras, and more complex vein recognition, biometric gait recognition, and voice recognition.

The suggested user identity verification approaches have some serious security flaws. Sentry sensor are used to detect the occurrence of an interest event, which then works as a trigger to wake up other sleeping sensors and allow them to participate in event monitoring. This approach was proposed as a means to increase the energy efficiency of smart daycare sensors; however, it contains a single point of failure that prevents it from being effectively applied in a safe smart daycare setting. All other monitoring sensors will stay dormant if attackers can locate and manipulate the sentry sensors, and the entire smart daycare may be hacked. For many years, inhabitant behavior prediction has been frequently employed in the assisted living setting.

Researchers such as Zheng et al (2008) used vibration sensors to detect a person falling or interacting with various objects, modified pyroelectric infrared sensors to detect stove and oven operations in the kitchen, multiple Ultrasonic sensors to identify inhabitant locations inside the daycare, and pressure sensors to detect the presence of a user, steps taken by the user, and identify the user. Although light sensors or photo sensors were not widely utilized for behavior prediction, they were employed to detect user presence in various sections of the daycare and to measure direction.

Some approaches used magnetic switches to identify the status of a door or a cupboard at various parts of the daycare.

Microphones were utilized by Fleury et al. (2010) to recognize numerous user behaviors in a home, such as talking, door shutting, walking, phone ringing, things dropping, and TV viewing. Various researchers advocated the use of a Wattmeter to detect energy use in the home, which is now regarded as a key measure of an inhabitant's well-being. Most of these methods identify a user's unique action in a specific section of the home, thus using them to detect infiltration attempts in a smart daycare would be wasteful.

Intruders cannot always be expected to utilize the kitchen or another specialized area of the home; moreover, most of these proposed techniques require time to differentiate between normal and assault behavior, which is limited in a security situation.

Over the years, researchers have suggested many techniques for activity detection utilizing wearable sensors. Activity recognition may be done with accelerometer data. Wannenburg & Malekian (2016) proposed the use of smartphone accelerometer data to detect user behaviors including running, walking, standing, sitting, lying down, and so on. The smartphone is kept in the user's trouser pocket during the observation.

They later developed an optical pulse oximeter sensor and coupled it with a digital temperature sensor to create a wearable gadget that could monitor heart rate, oxygen saturation, pulse transit time, and skin temperature to detect medical stress.

Merilahti et al. (2009) proposed using a wrist-worn activity detector to determine if a user is sleeping or awake. To simulate user rhythms and behavior, Van Laerhoven et al. (2008) integrated accelerometers, tilt switches, and inertial sensors into a wrist-worn sensing device.

Maekawa et al. (2013) used hand-worn magnetic sensors to detect and discriminate between distinct magnetic fields generated by different electrical equipment in the home, as well as recognizing user activity. Wearable sensors are used to identify user behavior at home; however, they are inconvenient for the users because they must wear them all the time. Furthermore, given human nature of forgetfulness and carelessness, it will be difficult to apply properly.

Sensors installed in smart daycares may be used to anticipate user behavior within a home, according to Dawadi et al. (2016), this behavior data can be used to predict an individual's clinical ratings. According to the research, there is a link between a user's behavior as tracked by smart daycare sensors and his cognitive/physical health. To compute the clinical scores, the researchers analyzed sensor data to determine resident's sleep, cook, eat, relax, personal hygiene, and bed toilet changeover durations.

Paavilainen et al. (2005) examined different characteristics in the home, such as sounds generated during various tasks, position of the home's residents, inhabitant's speech, water consumption, light conditions, temperature, and so on, to determine user's everyday activities such as sleeping, cooking, and relaxing. The system uses microphones placed throughout the house to pick up noises and receive voice instructions; the sounds are then analyzed and preserved in order to understand human behavior, which may be considered a breach of privacy.

Tapia et al. (2004) centered their work on automated homes on recognizing users' everyday behaviors such as sleeping, eating, and so on. To enhance a home's efficiency, the suggested system employs supervised algorithms, training data, and user interactions to recognize and anticipate human behaviors. The recommended solutions were largely focused on increasing home efficiency and placed a low priority on home security. Furthermore, they have a high

computational overhead and necessitate expensive hardware through supervised and unsupervised learning, human behavior can be learnt and predicted. Unsupervised learning necessitates data annotation, which is a time-consuming procedure. Kasteren et al. (2009) used Hidden Markov models (HMMs) to recognize user behavior in their study. Zheng et al (2008) used neural networks and Doctor et al (2012) used fuzzy logic to learn and model actions in the iDorm unsupervised.

Mihailidis et al. (2004) looked at how users washed their hands to detect their actions and behavior. Wu et al. (2006) recommended using a variety of tagged objects that the user regularly uses to detect and model user behavior.

To enhance performance, Aztiria et al (2008) exploited user input. When using behavior prediction to detect infiltration attempts in a home security scenario, human intervention is not always possible. To detect intrusion, the algorithm proposed in this study uses minimal user interference.

Monekosso & Remagnino (2010) used a Hidden Markov Model to analyze activities such as cooking, eating, bathroom/ablutions, watching TV, sleeping/in bed, working at a desk, or no observable activity to find patterns in observed data.

Mokhtari et al. (2017) employed pyroelectric infrared sensors to identify the direction in which a user is moving inside a residence**,** and an ultrasonic array to determine the height of a moving resident; both of these pieces of information are merged to compute the velocity at which someone travels. For data transmission to the data server, the researchers used Bluetooth Low Energy (BTLE) communication models.

The study focuses on distinguishing home inhabitants from one another based on their physical characteristics and the pace with which they move throughout the home, so the system only has to discriminate between a few home residents. When this method is used in home security, the sample set is considerably larger. Also, velocity and physical attributes such as user height are insufficient to properly identify home intrusion

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter discusses the research design, study population, sampling technique, sample size, ethical considerations as well as validity and reliability. It also describes and justifies the methods and processes employed in the collection and analysis of data. Again, it describes the proposed smart daycare architecture model/system. It further describes the architecture of the smart daycare model, the Central Management Unit (CMU) components and some examples in smart daycare situation / scenarios.

3.2 Research Design

A research design is a conceptual framework for conducting research; it serves as the blueprint for data collection, measurement, and analysis (Leavy, 2017). According to Saunders, Lewis, & Thornhill (2012), the choice of any study design is based on a number of factors, the most important of which are the characteristics of the variables or population being utilized or examined. A research design, according to Cohen, Manion, & Morrison (2011), is an overall strategy for getting answers to the questions being investigated as well as for dealing with some of the challenges that may arise during the research process.

According to Creswell and Plano (2011), the kind of data, the data collection technique, the sample strategy, the schedule, and the budget are all determined by the research design. They also stated that a good study design aids in aligning the intended technique with the research questions. Because different research designs seek to address different sorts of research

problems, the research design chosen must be based on the nature of the study, its context, potential restrictions, and the study's underlying paradigm. This study aims at achieving a secure internet of things using a smart daycare architecture model/system for a smart daycare environment. It also identifies the potential security threats and possible relating consequences, solution and recommendations for the implementation of this system, the extent of need of smart daycare system implementation and the effectiveness of the system for effective teaching and learning; hence, the research approach used for this study was descriptive. According to Creswell and Plano (2011), descriptive research is used to explain a situation as it occurs naturally. It can be used to support current practice and/or make a subsequent judgment, as well as to create hypotheses. According to Saunders, Lewis, and Thornhill (2012), descriptive research is a form of definitive research study focused on defining the features of a certain individual or group. By using the descriptive research design, the researcher attempts to obtain complete and accurate information concerning the extend of need of the IOT based smart daycare system architecture, some security threats associated with its implementation in a daycare environment and the effectiveness of the system for teaching and learning.

In addition, the descriptive research approach was chosen for the study because it is suitable and useful for identifying existing situations and pointing to current requirements (Creswell & Plano, 2011). Other reasons for using descriptive research design include:

- Determines and reports the way things are;
- Involves the collection of data in order to test research questions concerning the current status of the subjects of the study;

- Makes it feasible to observe, explain and document aspects of a given situation as it naturally occurs.

3.3 Study Population

The whole collection of subjects that may be researched is referred to as a population (Oppong, 2013). According to Oppong, defining the study's target group is critical since it aids the researcher in making decisions about sampling and resources to utilize.

The target population for this study was teachers and parents of children at Winners Academy daycare, Future Leaders daycare and Mount Zion International daycare all in the Lambussie District. Winners' academy has a staff strength of twenty (20) with a total student enrolment of 450. Future leaders and mount Zion international school has a staff strength of 25 and 15 with a total student enrolment of 520 and 280 respectively. In all, they have a student population of 1,250 and a staff population of 60 in the three schools. All these students have parents who care much about the safety and security of their wards in school.

3.4 Sampling Technique

As Oppong (2013) pointed out, sampling is unavoidable in research since surveying the complete population is impractical owing to budget and time restrictions, consequently, samples are drawn to appropriately represent a population. A sample, according to Bryman (2012), is a small group of units used to draw broad generalizations about the total. Its main goal is to offer reliable estimations of a parameter that is unknown. It's made up of individuals or units. According to Saunders, Lewis, and Thornhill (2012), the processes entail selecting a sample from a large list of sampling units. In practice, a true list is seldom found, therefore a comparable list is used

instead. For some study questions, it is feasible to solicit information from an entire population as it is of a controllable size.

A non-probability sampling technique was used in this research. Non-probability sampling methods, according to Bryman (2012), give the researcher a variety of options to choose from. The stratified, purposive, and convenient sampling procedures were used for the purposes of this research. With the stratified sampling, the researcher sampled the population into male, female, parents and teachers to ensure that the sample reflects each stratum sorted based on gender, parents and teachers. Afterwards, the simple random sampling was used on each stratum to select 82 males and 68 females as well as 100 parents and 50 teachers constituting a representative sample of 150 participants in both cases. In the case that one or more strata in the population have a low incidence compared to the other strata, stratified sampling guarantees fair representation. Also, the purposive sampling was used to get the required representative number of teachers and parent for the study. The researcher visited the various schools and homes of some parents and purposefully selected teachers and parents who were accessible at the time of his visit since only teacher and parents were the focus groups for the study. They were purposefully selected because they have a clear criteria and rationale for inclusion and generalization. The study also described in details how the IOT bases smart daycare system operates. With the convenient sampling, because schools were in session at the time of his visits, teachers who were available but not accessible and have been purposefully selected were given the questionnaire to fill at their convenience and submit at a later date. Also, some parents were also given copies of the questionnaire to answer at their convenience and were collected at an agreed date.

3.5 Sample Size

A total of 150 participants from the selected institutions were selected to take part in the study. Gentles (2015) claims that if a basic method is performed correctly, a sample size of 150 - 200 research participants may be regarded appropriate and represents the entire population. This supports the sampling size selection. Saunders, Lewis, and Thornhill (2012) said that the sample size should be 100 or greater as a general rule. The sample of 150 is made up of 100 parents and 50 staff from the various institutions.

3.6 Data Collection Instrument

The purpose of this study was to obtain quantitative data using close ended questionnaire. The word "questionnaire" is used to refer to any data collection procedure in which each individual is obliged to answer the same set of questions in a preset order (Saris & Gallhofer, 2014). Questionnaires are one of the most common types of primary data collection that is used to ensure data accuracy. In more than half of all comprehensive research studies in education, it is a common approach for obtaining primary data. A valid questionnaire will allow for the collection of accurate data, and a trustworthy questionnaire will ensure that these data are gathered consistently (Sreejesh & Mohapatra, 2014). Respondents were required to provide response to various questions using the five (5) point Likert scale based on their satisfaction. This study used a scale of 1 – Large Extent, 2- Some Extent, 3- Undecided, 4 – Less Extent, 5 No Extent. Also, respondents were expected to tick the box which best reflects their view. Again, using the questionnaire guaranteed that responses were consistent, homogeneous, and stable. It also

allowed respondents to complete the questionnaire at their leisure, while also ensured better anonymity for the respondents using closed ended questions.

3.7 Data Sources and Data Collection Procedures

In educational research, there are two sources of data: primary and secondary sources (Sekaran & Bougie, 2010). Both sources of data were used to compile the data for this study. A primary source (Sreejesh & Mohapatra, 2014) is an original document or narrative that stands alone and is not about another document. For instance, surveys based on participants' responses to standardized questions (Guest, Namey, & Mitchell, 2013). A researcher can use primary sources to come as near to what truly happened during a historical event or era as feasible.

A secondary source, on the other hand, is made up of material that cannot be defined as original source data and does not have a direct physical link with the event being investigated (Saunders et al., 2012). A secondary source is one in which the person recounting the event was not there but acquired a description from another person or source, such as textbooks or quoted materials. Secondary sources of data, according to Saunders et al. (2012), are typically of limited value due to the mistakes that occur when information is transmitted from one person to another. Nevertheless, Secondary data sources are still important in educational research. Secondary sources, according to Bryman (2012), should not be overlooked. Because education is primarily concerned with the individual's physical, social, and intellectual development, there are several situations when a secondary source can substantially contribute to more legitimate and reputable sources than would otherwise be the case. According to Flick (2011), data from many sources will be used to get the essential information and answer the study questions. They will supply

abundant sources of specific information and guarantee that the findings are validated through triangulation by working together. First of all, the researcher administered some few questionnaires to a small sample of the population as a pilot. This after analyses, the results proved to the researcher that the instrument to be used was valid, reliable and appropriate to the study.

Furthermore, the researcher visited the various daycare schools to meet and interact with the teachers about the purpose of the research. A few of the teachers were busy but majority of them were available and ready to support. Questionnaires were administered to all the teachers present. Those who were able to finish, submitted the same day, however an opportunity was given to some teachers who may want to take it home due to their busy schedules but returned it the following day. Also, the researcher visited most parents of kids in the evening because it was in the raining season where they either went to work, market or farm. At the end of the exercise, 95% of the questionnaires were retrieved.

3.8 Pilot Study

A pilot study of the questionnaire was done in FIC Jubilee international Daycare using 30 participants comprising 20 Teachers and 10 Parents. This school was not used for the study. That was done to ensure that the research instrument was devoid of ambiguities, spelling mistakes and grammatical errors. The Cronbach's coefficient alpha, which is normally used to establish the internal reliability of questionnaires, was used to determine the reliability coefficient of the questionnaires. The questionnaire had a reliability coefficient of 0.73 which indicated that it was useful for the study (de Vaus, 2002).

3.9 Ethical Considerations

According to Dick & Pedersen (2013), Ethics in research is involved with what is right and what is not right to do when conducting research and forms an integral part of any research study. The issue of ethics in research is particularly important when human beings are the research subjects as is the case in this study (Hammond & Wellington, 2012). According to Dick & Pedersen (2013), ethics in research spans the entire research process, from the nature of the problem being investigated, the reporting of the theoretical framework thereof, the context within which the research is conducted, the data collection instruments employed, the data collection methods used, the research subjects, the procedures employed to analyze the data and the way in which the data is reported. In line with this, measures were taken to ensure that respondents and any participant in this research work was not harmed in any way.

The researcher did not include any participant without their approval or consent. Permissions was sought, and the aims and objectives of the study were made known to the appropriate Participants and all other respondents before the questionnaires were administered. All participants were assured that the study is for academic purposes only. Participants were not forced but instead were urged to participate voluntarily. All information gathered from the study are being kept well and treated as confidential.

3.10 Data Analysis

In methodology literature, there is not one single right way or the most appropriate way to analyze quantitative data. Analysis implies and indeed requires an ultimate choice (Sekaran & Bougie, 2010). For instance, in analyzing and interpreting quantitative data, it is the process of

systematically organizing the materials collected, bringing meaning to them so that they tell a coherent story and writing it all up so that others can read what one has learnt. Based on this premise, the data collected was analyzed using quantitative methods to enable the researcher to provide a reasoned meaning to the study. Consequently, the responses were edited, coded and scored. The scores for each respondent were summed across the items to obtain their final raw score. Simple percentages and frequency tables as well as regression analysis were used to examine the issues. In a few cases, the mean of means was used to analyze the specific variables. This analysis was done based on each research question.

3.11 Validity and Reliability

Validity is the ability of an instrument to measure what it is supposed to measure. According to Flick (2011), the interpretation of validity has two (2) components, which includes whether the instrument truly measures the idea in question and whether the idea is measured precisely. Validity suggests the extent to which an instrument is performing what it is designed to perform, and numerous sources provide evidence of validity. The validity of the research instrument was evaluated for content and construct validity.

3.11.1 Content Validity

Content validation can be undertaken by the researcher alone or with the assistance of others (Flick, 2011). The content validity of the questionnaire to adopt in the research was determined by the literature review as well as by the judgment of the researcher.

3.11.2 Construct Validity

Construct validity is more concerned with the underlying attribute than with the scores that the instrument produces. Its significance is in its linkage with theory and theoretical conceptualization (Zohrabi, 2013). It concerns validation of not just the instrument but also the principles underlying it (Kimberlin & Winstertein, 2008). Heale & Twycross (2015) define reliability as the degree of consistency with which an instrument measures the characteristics it is intended to measure. They explain that reliability is primarily concerned not with what is being measured but with how well it is being measured.

The reliability of a measuring tool can be assessed in several ways. The approach to be adopted depends to a specific extent on the nature of the instrument but also on the aspect of the reliability concept that is of most significant interest. The aspects that will receive significant attention are stability, internal consistency, and equivalence (Kimberlin & Winstertein, 2008). The stability of a measure relates to the degree to which the related outcomes are achieved on replicated administrations of the same instrument. (Heale & Twycross, 2015) maintain that the internal consistency approach to estimating an instrument's reliability is probably the most widely used method among researchers today. Research experts and supervisors usually assess the instrument and the homogeneity of the variables before it is used. Reliability will be further be ensured through conducting a pretest.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

This chapter deals with the results and discussion of the findings based on the research objectives. This study gathers information concerning the extend of need/use of the IOT based smart daycare system architecture, some security threats associated with its implementation in a daycare environment and how the proposed system affects teaching and learning. It also discusses the principles of IOT smart daycare systems model, compliance with existing infrastructure and communication standards, how it operates, consistent power supply and potential security threats. The target for this study will be teachers and parents of children at Winners Academy daycare, Future Leaders daycare and Mount Zion International daycare all in the Lambussie District.

4.2 Response Rate

The researcher issued questionnaire to 60 teachers and 120 parents, thus a total of 180 respondents. Questionnaires from 56 teachers (93.3% return rate) and 114 parents (95.0% return rate) were returned. Therefore, the study realized an instrument return rate of 95.6%, which was very satisfactory for the purpose of the study which is in line with Mugenda & Mugenda (2003). This efficient response rate was realized since the researcher personally administered the questionnaires, created rapport with the respondents and collected the instruments immediately after they were completed. According to Edwards et al (2002) a response rate of less than 60 percent is considered inadequate while that of 60.0% percent to 80.0% is adequate. In addition,

if the response rate is over 80 percent, it is considered as excellent for the purpose of a study/research.

4.3 Demographic Information of Respondents

This researcher first sought to find out the gender, and age distribution of the respondents to establish an insight on the demographic characteristics of respondents. To find out respondent's characteristics in regard to gender, the researcher sought to establish teachers and parents gender distribution. The findings were presented as shown in Table 4.1.

Table 4.1: Gender Distribution of Respondents

Sex	Frequency (N)	Percentage (%)
Male	82	54.7
Female	68	45.3
Total	**150**	**100.0**

Source: Field Work, 2021

Table 4.1 shows that both males and females were captured in the study.

Data from the table indicates the sex composition of the respondents who took part in the research. Out of the 150 respondents, 82 of them representing 54.7% were males whereas 68 of the remaining respondents representing 45.3 % were females. This implies that majority of the respondents in the study were males. The researcher further sought to find out respondents age bracket and presented the findings as shown in Table 4.2.

Table 4.2 Age Category of Respondents

Age	Frequency (N)	Percentage (%)
Below 30 years	52	34.7
30-35 years	28	18.7
36-40years	23	15.3
41-45 years	21	14.0
Over 45 years	26	17.3
Total	**150**	**100.0**

Source: Field Work, 2021

Table 4.2 clearly shows that the respondents were fairly distributed among the age brackets set out for the questionnaire. As indicated in Table 4.2, 52 (34.7%) of the respondents were below 30years; 28 (18.7%) of the respondents were between the ages of 30-35years; while, 23 (15.3%) of the respondents were between the ages of 36-40years; and 21 (14.0%) of the respondents were between the ages of 41-45years as well as 26 (17.3) of the respondents were above 45 years. This implies that majority of the respondents who participated in the research were below 40years and therefore are at their youthful age consisting of parents and teachers. Also, the data is spread across all the categories of age groups, that is young, middle age and old (45 years and above). This therefore caters for all the age interest needed for the study.

Analysis on Objective One (1).

4.4 Extent of Need/effectiveness of IOT Based Smart Daycare System Implementation in a Daycare Environment

Under this section, the parents and teachers were asked to indicate the extent to which smart daycare system deployment was needed and how effective it will be to improving child security and teaching and learning in the selected daycare schools

in the Lambussie District. Presented in Table 4.3 and Table 4.4 are the responses gathered from the parents and teachers respectively.

4.4.1 Teachers extent of Need of Smart Daycare System in Schools

Table 4.3 presents the extent to which the teachers need the smart daycare system. The mean of the variables under consideration was computed. The computed means were compared with the predetermined mean of 3.0.

Table 4.3: Responses on Teachers Extent of Need of Smart Daycare System to Promote Teaching and Learning and Child Security in School

S/N	Teachers' extent of need of smart daycare system	Mean	Std. Dev.	Decision
	The need for Smart daycare system for working independently and self-directed			
1.	Teachers need the system to work independently through sensors	3.43	1.182	Large extent,
2.	Teachers need the system to adjust to its usage	3.21	1.253	Large extent
3.	Teachers need the alarm system component to organize students	2.65	1.310	Small extent
4.	Teachers are not ICT literates and may find it difficult to adjust to its usage	2.54	1.277	Small extent
	Smart daycare system for safety and security of kids			
5.	Teachers need the system to monitor student movement	3.19	1.469	Large extent
6.	Teachers need the system to protect school property	2.50	1.271	Small extent
7.	Teachers need the system to prevent unlawful intruders	2.85	1.416	Large extent
	Smart daycare system for learning and understanding			
8.	Classroom contains interactive smart devices to enhance learning	3.77	1.220	Large extent
9.	Teachers need the system to introduce more technology tools to kids.	3.61	1.399	Large extent
10.	Most teachers need adequate knowledge in the use of the system devices when implemented	3.55	1.464	Large extent

	Smart daycare system for contact out of class			
11.	Teachers need the system to check register of attendance	3.17	1.511	Large extent
12.	Teachers need the system to regularly communicate with parents	2.59	1.289	Small extent
13.	Teachers need the system to work collaboratively with their colleagues and parents	2.03	.897	Small extent

Source: Field Survey, 2021 *Mean ≥3.0=Large Extent* *<3.0=Small Extent*

4.4.2 The Need for Smart Daycare System for Working Independently and Self-Directed

As depicted in Table 4.3, Teachers need the system to work independently through sensors was highly scored. This statement had a mean score of 3.43 and a standard deviation of 1.182. This means that, the system upon full implementation will enable teachers to work independently and self-directed through sensors and other system components.

With a mean score of 3.21 and a standard deviation of 1.253, the study indicated that Teachers need the system to adjust to its usage. Again, with a mean of 2.65 and a standard deviation of 1.310, the teachers to a small extent need the alarm system component to organize and control students during instructional period such as break, closing, assembly and many others.

On the other hand, some teachers to a small extent Teachers are not ICT literate and may find it difficult to adjust to system usage with a mean of 2.54 and a standard deviation of 1.277.

4.4.3 Smart Daycare System for Safety and Security of Kids in School

It can be observed from the study results in Table 4.3 that, teachers to a large extent need the smart daycare system to monitor student's movement in school with a mean score of 3.19 and a standard deviation of 1.469. This implies that school administrators/teachers need the system to effectively monitor students during instructional period. On average, teachers to a small extent need the system to protect school property. This is supported by a mean of 2.50 and a standard deviation of 1.271. Moreover, teachers to a large extent need the system to monitor and prevent unlawful intruders. This statement was reflected by a mean of 2.85 and a standard deviation of 1.416. This means that, the system is needed to ensure safety and security of kids in school when fully implemented.

4.4.4 Smart Daycare System for Learning and Understanding

Data collected reveals that, teachers need the smart daycare system to enhance leaning and understanding. Statistically, the study indicates that classrooms contain interactive smart devices to enhance learning. This is supported by a mean of 3.77 and a standard deviation of 1.220. Again, teachers to a large extent need the system to introduce more technology tools to actively engage kids in class with a mean of 3.61 and a standard deviation of 1.399. This corresponds to approximately 2nd on a Likert scale implying that most of the teachers really need the system implementation to positively impact learning. Moreover, most teachers to a large extent need adequate knowledge in the use of the system devices with a mean of 3.55 and standard deviation of 1.464.

4.4.5 Smart Daycare System for Contact Out of Class

It can be observed from the study results in Table 4.3 that, teachers to a large extent need the smart daycare system to check register of attendance of kids. This statement reflected a mean of 3.17 and a standard deviation of 1.511. This implies that most of the teachers/administrators need the system to keep attendance of kids each day. Moreover, teachers to a small extent need the system regularly communicate with parents of kids with a mean score of 2.59 and a standard deviation of 1.289. Furthermore, the study indicated that teachers to a small extent need system to work collaboratively with colleagues and students. This is supported by a mean of 2.03 and standard deviation of .897 implying that most of the teachers need the system to communicate and collaborate with each other as well as students.

4.5 Effectiveness of Smart Daycare System use by Teachers towards Improving Teaching and Learning in Schools

In order to evaluate the effectiveness of smart daycare system on effectiveness of teaching and learning in daycare schools, the variable for effectiveness of smart daycare system use by teachers was conducted.

4.5.1 Effectiveness of Smart Daycare System Implementation by Teachers

Table 4.6 addresses the effectiveness of smart daycare system implementation by teachers in daycare educational institution.

Table 4.4: Response of Teachers on Effectiveness of Smart Daycare System Implementation in Enhancing Teaching and Learning and Security of Kids

S/N	Effectiveness of smart daycare system implementation by teachers to enhance Teaching and learning and kids' security.	Mean	Std. Dev.	Decision
	Effective in working independently and self-motivated			
1.	Teachers are more effective in using the system devices to monitor kids	3.89	1.002	Agreed
2.	Teachers are more effective in controlling student movement on campus	3.64	1.183	Agreed
3.	Teachers are more effective submitting work on time.	3.52	1.339	Agreed
4.	Teachers are more effective organizing their work	3.25	1.622	Agreed
5.	Teachers are more effective in training students to use smart devices for learning.	3.14	1.296	Agreed
6.	Teachers are more effective working independently	2.22	.900	Disagreed
	Teachers to develop knowledge effectively			
7.	Teachers are more effective in developing their understanding on system operation.	4.58	.901	Agreed
8.	Teachers are more effective reinforcing their knowledge	4.32	.915	Agreed
9.	Teachers are more effective engaging with the kids in class	3.46	1.464	Agreed
10..	Teachers are more effective managing students using the system after school	2.18	1.052	Disagreed
	Access information and communicate effectively			
11.	Teachers are more effective using GSM/mobile based daycare automation for communication.	4.48	.844	Agreed
12.	Teachers are more effective contacting parents of kids	4.51	1.015	Agreed
13.	Teachers are more effective monitoring students from outside class	3.42	1.356	Agreed
14.	Teachers effectively have peace of mind to interact with kids	2.55	1.297	Disagreed
15.	Teachers are always busy in using the CCTV cameras.	2.25	.920	Disagreed
	Research and present information effectively			
16.	Teachers are more effective presenting assessment electronically	4.32	1.147	Agreed
17.	Teachers are more effective in using internet-based daycare system for communication	4.17	1.356	Agreed
18.	Teachers are more effective researching topics	2.18	1.301	Disagreed

Source: Field Survey, 2021 ***Agreed: ≥ 3.0, Disagreed: < 3.0***

4.5.2 Effective in Working Independently and Self-Motivated

From Table 4.4, it appeared that Teachers are more effective in using the smart daycare system to monitor kids in school with a mean of 3.89 and a standard deviation of 1.002. This implies that smart daycare system implementation by Teachers ensure effective monitoring by the teachers. Again, the study indicated that Teachers are more effective in controlling student movement on campus. This is supported by a mean of 3.64 and a standard deviation of 1183. Moreover, Teachers are more effective in submitting work/documents to management on time with a mean score of 3.52 and a standard deviation of 1.339.

In addition, the teachers agreed that smart daycare system will make teachers more effective organizing their work with a mean score of 3.25 and a standard deviation of 1.622. Also, the teachers indicated that smart daycare systems are effective in training students to use smart devices for learning. This is supported by a mean of 3.14 and a standard deviation of 1.296. Again, the statement that teachers are more effective working independently had a mean of 2.22 and a standard deviation of .900 which was disagreed.

4.5.3 Effective in Making Teachers Develop Knowledge

As displayed in Table 4.4, teachers are effective developing their understanding on system operation with a mean of 4.58 and standard deviation of .901. This implies that most of the teachers tries to understand the components of the system and how they operate. Again, the teachers agreed that, they are more effective reinforcing their knowledge on the system. This statement had a mean of 4.32 and a standard deviation of .915. Also, Teachers are more effective engaging with the kids in class. This is supported by a mean of 3.46 and a standard deviation of 1.464. this implies that, with

the smart daycare system implementation, teachers are able interact effectively with kids in class using technology tools. This arouses their interest in class since they are allowed to feel what they learn. Concerning the statement that, Teachers are more effective managing students using the system after school, teachers disagreed to this statement with a mean of 2.18 and a standard deviation of 1.052.

4.5.4 Effective Access to Information and Communication

The data from the study reveal that most of the teachers are effective in using the GSM/mobile based daycare automation for communication. This is supported by a mean of 4.48 and a standard deviation of .844. Teachers are more effective contacting parents of kids using the system. This has a mean of 4.51 and a standard deviation of 1.015. Furthermore, the teachers agreed that adoption of smart daycare system makes it easy for teachers to monitor students from outside class on the school compound. This statement had a mean of 3.42 and standard deviation of 1.356. The statement that smart daycare system makes teachers to have peace of mind to interact with kids had a mean of 2.55 and a standard deviation of 1.297. Again, the statement that teachers are more effective in using the CCTV cameras have a mean of 2.25 and a standard deviation of .920.

4.5.5 Research and Present Information Effectively

It can be observed from the study results in Table 4.4 that Teachers are more effective presenting assessment results of kids electronically with the smart daycare system. This statement had a mean of 4.32 and a standard deviation of 1.147. This implies that most of the respondents agreed on effectiveness of smart daycare system for presenting assessment results of kids. Again, teachers are more effective in using internet-based daycare system for communication. This is supported by a mean of 4.17 and a standard deviation of 1.356. However, the statement that smart daycare

system makes teachers and kids more effective in researching topics had a mean of 2.18 and a standard deviation of 1.301.

4.6 Extent of Need of Smart Daycare System Implementation

Under this section, parents were asked to indicate the extent of need of smart daycare system implementation. Table 4.5 presents the responses from parents on the extent of need of smart daycare system implementation in the various daycare schools to monitor the safety and security of their kids in school. The variables under consideration were computed.

Table 4.5: Extent of Need of Smart Daycare System Implementation by Parents towards Improving the Security of Kids

S/N	Extent of need of smart daycare system by parents	Mean	Std. Dev.	Decision
	Smart daycare system for child safety and security			
1.	Parents need the system to enhance confidence on the safety of their kids	4.29	1.057	Agreed
2.	Parents need the system to collaborate with teachers to ensure security of kids	4.25	1.031	Agreed
3.	Parents are concerned about the security challenges of the system	3.95	1.367	Agreed
4.	Parents will be notified on how kids are coping up learning.	3.73	1.421	Agreed
	Smart daycare system for access to information and progress of kids			
5.	Parents need the system to be able to track progress of their kids	4.34	1.083	Agreed
6.	Some parents may feel reluctant to visit kids in school due to enhanced security by the system	4.14	1.285	Agreed
7.	Students will get to understand what is being taught	4.09	1.269	Agreed
8.	Parents need the system to for update on child welfare issues	3.00	1.250	Agreed

Source: Field Survey, 2021

4.6.1 Smart Daycare System for Child Safety and Security

The table above reveals that parents need the system to enhance confident on the safety of their kids after adopting the smart daycare system. This statement had a mean of 4.29 and a standard deviation of 1.057. Again, Parents need the system to collaborate with teachers to ensure security of kids. This is supported by a mean of 4.25 and a standard deviation of 1.031. Moreover, the Parents are concerned about the security challenges of the system. This statement had a mean of 3.95 and a standard deviation of 1.367. Again, with a mean score of 3.73 and a standard deviation of 1.421, parents will be notified on how kids are coping up in school.

4.6.2 Smart Daycare System for Access to Information and Progress of Kids

From Table 4.5, the parents indicated that by implementing smart daycare system, Parents are able to track progress of their kids through the system in collaboration with teachers. This statement had a mean score of 4.34 and a standard deviation of 1.083. Moreover, some parents may feel reluctant to visit their kids in school due to enhanced security. This is supported by a mean of 4.14 and a standard deviation of 1.285. An indication from Table 4.5 reveals that Students get to understand what is being taught. This statement reflected a mean of 4.09 and a standard deviation of 1.250. However, parents need the system to be updated on child safety and security more effectively through the system. This statement had a mean of 3.00 and a standard deviation of 1.250.

Analysis on Objective Two (2)

4.7 Potential Challenges and Security Threats Associated with the Use of IOT Based Smart Daycare System Architecture

This section depicts some potential challenges and security threats associated with the implementation of the smart daycare system in Ghana. The respondents were asked to indicate the extent to which they agreed with each statement. The table 4.6 below shows the challenges/security threats associated with the implementation of IOT based smart daycare system in Ghana.

From the table below, it is observed that interruption of the system by electricity posed a challenge to the implementation of the smart daycare system, both Teachers (M=3.60, SD=1.217) and parents (M= 3.39, SD= 1.545) agreed to this statement. This indicates that interruption of electricity supply in the Lambussie District affect Teachers access to the system. Results in the pilot study confirmed this statement. (Montrieux, et al., 2015; Richard & Haya, 2009) reported from other developing countries show similar results that lack of electricity supply affects the successful implementation of the smart daycare system.

The issue of Computer network failure during communication affects successful execution of the system, teachers (M=3.39, SD=1.393) and parents (M=3.14, SD=.1.519) agreed to the statement.

Furthermore, both teachers (M=3.18, SD=1.285) and parents (M=3.30, SD=1.513) agreed that lack of basic and adequate infrastructure/ resources affect effective implementation of the system.

Regarding the spoofing and phishing attacks on system data and resources, both teachers (M=3.09, SD= 1.273) and parents (M=3.39, SD=1.397) agreed to the statement. This means that they may be several spoofing and phishing attacks on the

system which can affect the successful operation of the system. Therefore, there is the need to ensure that the system has no vulnerabilities by strengthening the security components. Also, they may be virus and spyware threats in the system if the security of the system is not monitored regularly.

On the contrary, both teachers(M=2.79, SD= 1.201) and parents (M=2.84, SD= 1.462) disagreed that smart daycare implementation is time consuming, inadequate knowledge on how to use the smart daycare system for teachers(M=2.46, SD=1.270) and parents(M=2.29, SD=1.514), attacks by hackers and predators to gain access to unauthorized data for teachers(M=2.34, SD=1.120) and parents(M=2.32, SD=1.428), lukewarm attitude of some parent towards child welfare and safety for teachers(M=2.12, SD=.942) and parents(M=2.25, SD=1.240), lack of ICT technicians and personnel for teachers(M=2.11, SD=1.037) and parents(M=2.55, SD=1.476), as well as insufficient funds to upgrade and maintain the equipment and facilities for teachers(M=2.10, SD=1.072) and parents(M=2.52, SD=1.335) affects the successful implementation of smart daycare system at daycare schools in Ghana. These statements failed to meet the predetermined cut-off point of 3.0 as shown below;

Table 4.6: Responses on the Potential Challenges and Security Threats Associated with the Implementation of Smart Daycare System by Teachers and Parents

S/N	Challenges and security threat associated with smart daycare system	Teachers		Parents	
		Mean	Std. Dev.	Mean	Std. Dev.
1.	Interruption of the system by electricity	3.60	1.217	3.39	1.545
2.	Computer network failure	3.39	1.393	3.14	1.519
3.	Lack of basic and adequate infrastructure/ resources	3.18	1.285	3.30	1.513
4.	Spoofing and phishing attacks on system data and resources.	3.09	1.273	3.39	1.397
5.	Usage of the system is time consuming	2.79	1.201	2.84	1.462
6.	Inadequate knowledge on how to use the smart daycare system	2.46	1.270	2.29	1.514
7.	Attacks by hackers and predators to gain access to unauthorized data.	2.34	1.120	2.32	1.428
8.	Lukewarm attitude of some parents concerning child welfare and safety	2.12	.942	2.25	1.240
9.	Lack of ICT technicians and personnel	2.11	1.037	2.55	1.476
10.	Insufficient funds to upgrade and maintain the equipment and facilities	2.10	1.072	2.52	1.335

Source: Field Survey, 2021 *Agreed: $\geq$ 3.0, Disagreed: < 3.0*

Analysis on Objective Three (3).

4.8 Regression Analysis

In order to address the last research question, regression analysis was conducted to find out the effect of smart daycare system on effectiveness of teaching and learning in daycare schools. The results are summarized and the original Table from SPSS-23.

4.8.1 Linear Regression Model Summary

The researcher analyzed the variations of effectiveness of teaching and learning due to the extent of the need of smart daycare system in daycare schools. The findings are shown in Table 4.7.

Table 4.7: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.543[a]	.295	.269	1.092

a. Predicators: (Constant), effective in working independently, effective in developing knowledge, effective in accessing information and communicate, effective in research and present information
Source: Field Survey, 2021

According to the model summary output, the variables were significantly correlated where R (coefficient of correlation) was a positive correlation of 0.543 indicating that the need of smart daycare system was highly related to effectiveness of teaching and learning and security of kids. The identified independent variables explain only 29.5% variation in the dependent variable (effectiveness of teaching and learning and child security). Analysis of variance was also carried out and the findings were presented in Table 4.8.

Table 4.8: Analysis of Variance

	Model	Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	54.330	4	13.583	11.393	.000[b]
	Residual	129.950	109	1.192		
	Total	184.281	113			

a. *Dependent Variable: smart daycare system need*
b. *Predictors: (Constant), effective in working independently, effective in developing knowledge, effective in accessing information and communicate, effective in research and present information*

The relationship was significant at critical value (0.001) since the reported p-value (0.000<0.01) was less than the critical value. This means that smart daycare system was significant at 95% confidence level on the model summary. This implies that smart daycare system has significant impact on the effectiveness of teaching and learning and child security (F=11.39, P=000<0.01).

4.9 Discussion of Results/Findings

After administering the questionnaire on the population, some results/findings were made in accordance with the research objectives and research questions. Responses were obtained on the extent of need of IOT based smart daycare system implementation in schools. Findings from the data reveals that;

Teachers need the system to enable them work independently/at their pace through sensors and other components. This indicates that most of the teachers at the daycare institution in Ghana to a large extent actually need an IOT smart daycare system to enable them work independently and self-paced, and also to organize and control kids towards ensuring their security. Similarly, Aboderin (2015) investigated the challenges and extent of smart daycare system need and adoption of a national policy

on smart daycare systems in Nigeria. The study recognized that smart daycare system influences teachers ICT competence. It found out that teachers use the system to work independently and remotely, submit assessment results and facilitate access to resources and services as well as remote exchange of information and collaboration.

It also indicated that some teachers to a large extent need the smart daycare system to enable them use system with ease. This finding can be buttresses with the study by Kirsh (2002) that, teachers need the e-learning component of the smart daycare system to organize their works and customize learning materials to meet the individual need of kids. However, to a small extent, Teachers are not ICT literate and may find it difficult to adjust with system usage and also, Teachers need the alarm system to organize students during break, assembly, closing and so on. Therefore, the researcher intends to organize training session for those teachers to enable them adjust to system usage and use the alarm system.

Also, with smart daycare system for safety and security of kid, findings indicate that teachers need the daycare system to a large extent to monitor student's movement and prevent unlawful intruders who may unlawfully enter the school compound. Also, the school property to a small extent is also protected since it concerns more on the safety of kids put under the control of teachers by their parents. From this analysis, it is a clear indication that the system to a large extent is needed to ensure the safety of kids in school.

Next, with smart daycare system for leaning and understanding, findings confirm that most of the teachers to a large extent need the smart daycare system to acquire and impact knowledge, engage with kids in class and work collaboratively with their peers in classroom. Rosenberg (2001) revealed that teachers can use the e-learning

component of the system to acquire and impact new skills or knowledge for the purpose of enhancing the kid's performance.

Again, with smart daycare system for contact out of class, teachers to a large extent need the system to check register/attendance of kids. This implies that most of the teachers need the system to keep electronic attendance of kids each day in the school.

Additionally, to achieve the objective that talks about the challenges and security threats associated with the use of IOT based smart daycare system, data collected revealed some findings. These findings indicate that, interruption of the system by electricity, computer network failure, lack of basic and adequate infrastructure/ resources, and phishing and spoofing attacks as well as virus and spyware attacks on system data and resources are some potential challenges/security threats associated with the implementation of the smart daycare system in Ghana. The finding agrees with the study conducted by Eze, Chinedu-Eze & Bello (2018) in Nigeria. According to the study conducted, teachers pointed out that bad quality of internet connection and difficulties accessing a computer/printer, poor electricity supply, poor organizational/management support affect successful implementation of smart daycare system.

On the issue of computer network failure, the findings agree with Alhomod and Shafi (2013) that computer network failure posed a challenge in the successful adoption of a system. Manir (2007) on the other hand affirmed that poor access to the Internet in Nigeria affects effective implementation of some components of the system(e-learning). Aboderin & Kumuyi (2013) also identified poor installation of system related facilities and devices, and irregular electricity/power supply as problems facing successful implementation of smart daycare management system in most localities in developing countries.

On the fact that lack of basic and adequate infrastructure/resources affects the successful implementation of the system, this implies that many daycare schools lack the infrastructure and resources to ensure smart daycare implementation. The finding concurs with the study by Anene et al. (2014). Anene et al. studied the problems and prospects of management system implementation in Nigerian schools by specifically examining availability of facilities and infrastructure for management systems as well as availability of materials and to ascertain if teachers actually need these materials such as e-learning, smart devices in their schools. They found out that one of the obstacles to management information system implementation was infrastructure deficiencies. The teachers lamented that most Nigerian schools do not have adequate infrastructure such as e-learning libraries, smart devices and as such, it affects online seminars or discussion with teachers, online examination and limited bandwidth.

On the effectiveness of smart daycare system implementation by teachers, the data collected revealed the following findings;

These findings indicate that smart daycare system implementation make teachers more effective in using the system to monitor kids, effective in controlling students' movement on campus, effective submitting work on time, effective in organizing their work and effective in training kids to use smart devices for learning in school.

It also confirmed that, with smart daycare system, teachers are able to work effectively in terms of document processing and other related tasks on time. The finding agrees with Mbarek & Zaddem (2013) that some smart daycare system components ensure effective solving of problems, effective for staff to work at their own pace, ensure some learners and teachers acquire innovative knowledge and skills to deliver data electronically at any time and from any place.

On the aspect of effectiveness of the system in making teachers develop knowledge,

findings reveal that IOT smart daycare system adoption makes teachers more effective in developing their understanding on system operations, reinforcing their knowledge on the system as well as other digital tools and engage actively with kids in class using technological tools.

On the effectiveness of the need of smart daycare for access to information and communication, the results confirm that, smart daycare system adoption is effective in the use of the GSM/mobile for communicating with parents of kids using the system through SMS and monitor students from outside class on the school compound using sensors. This will help to ensure a secure internet of things for safeguarding the safety and security of kids.

Also, on the fact of using the system for research and presentation of information effectively, findings revealed that the IOT smart daycare system implementation will enable teachers to be more effective in processing assessment results of kids electronically and effectively use internet-based daycare system for communication. The purpose of smart daycare system implementation is to enhance security and safety of kids to ensure quality of learning experiences and outcomes for learners. Again, another importance of smart daycare system implementation in our daycare schools is to create an environment where teachers are more effective processing assessment results of kids electronically and uses internet-based system for communication with parents.

Again, based on data collected on the extent of need of smart daycare system by parents, findings revealed that most parents are really interested and concerned in the safety and security of their kids by being confident on the security of their kids if the system is fully implemented, collaborate with teachers to ensure security and enhanced feedback from teachers on how kids are coping up with learning in school.

However, few parents are concerned about the security challenges/threats of the system.

Also, with smart daycare system for access to information and progress of kids, findings reveal that, adoption of smart daycare system helps parents to access updated information on the progress of kids, some parents may feel reluctant to visit kids in school, learners understand what is being taught in school and also parents are updated on the security and safety of kids through the GSM information system. This also confirms the results of the pilot study conducted.

Lastly to address the last research question, regression analysis was conducted to analyze the variations in the effectiveness of teaching and learning due to the extent of need of smart daycare system in schools. Findings from this analysis revealed that smart daycare system helped teachers to be more effective in working independently and self-motivated to work at their own pace, teachers developed their knowledge effectively and also helped teachers access information and communicated effectively on the progress and security of kids. On the other hand, parents needed smart daycare system for child safety and security and the access to information and progress of their kids in school. Findings agree with the study by Subhash (2018) who found a positive impact of smart daycare system for smart teaching and learning. The smart teaching and learning develop novel learning techniques among kids, advance teaching and learning experience, available online resources, motivates kids and ensure effective parent-teacher communication.

Also, Kirsh (2002) reported that the e-learning component of the IOT smart daycare system positively influences teaching and learning. Kirsh mentioned that the e-learning component provides consistent content, convenient and works anywhere and anytime for teachers and even some learners. The instructional materials are easily

updated and permits the use of multimedia which leads to reinforced learning through the use of video, audio, quizzes and other forms of interactions. Smart learning improve retention, provide immediate feedback and allows teachers to customize learning materials to meet the individual needs of kids (Robertson, 2000).

In conclusion, from the findings/results discussed above on the extent of need of smart daycare system implementation by teachers, challenges and security threats associated with the implementation of IOT based smart daycare system towards improving teaching and learning in school, effectiveness of smart daycare system implementation by teachers and the effect of smart daycare system on the effectiveness of teaching and learning, it is clear from the analysis that the study helped to identify and addressed potential security threats that may affect the smart daycare system, the study found out that, the system was much needed and necessary for both teachers and parents to enhancing the safety and security of kids and also has greater impact on effective teaching and learning of kids in school. This effectively ensured a secure internet of things based smart daycare system for a daycare environment.

4.10 Operations of the Smart Daycare System Model

The smart daycare system is made up of both hardware components as well as software. The software of the model is installed on a wired network with an internet access. The software monitors the overall actions and interactions of every motion at the daycare. Every child is registered unto the system together with whoever comes to pick up the child. Biometric details of both partners being the child and the care taker are taken and fed to the system which will serve as an authentication to give right for the person to take the child. Intruders are checked and monitored through the facial

recognition sensors which gives an alarm if it suspects an unrecognized person who is not registered onto the system by consulting the database of the system. The front cameras also check and monitors who is entering the premises of the daycare center.

4.11 Consistent Supply of Power

Power is necessary to keep smart daycare running and for that matter there should be a constant supply of power to our equipment and devices. In Ghana our major supply of power is the hydroelectric power which is not enough to rely on to successfully keep our smart daycare running and for that matter various options will be considered such as adoption of solar energy or stand by generators or plants which will be used to support the source of power supply to the devices and equipment that make up the smart daycare center.

4.12 Potential Security Threats Associated with IOT Based Smart Daycare Implementation in Ghana

As the smart daycare device sector of the technology market grows exponentially each year, more and more devices are being connected to the internet every day this assertion is by researchgate.net. Many of us find ourselves relying on this modern technology to assist us with our daily routines. However, connecting these devices to your networks can leave you vulnerable to cyberattacks if not properly secured.

According to researchgate.net on issues concerning security an estimated 80% of IoT devices are vulnerable to a wide range of attacks (Apthone et, al. 2017). Clearly, connecting traditionally ‘stand-alone’ smart devices such as lights, appliances and locks introduces numerous cyber security risks. Some security threats and attacks against smart daycare devices include:

4.12.1 Man-in-the-Middle

An attacker breaches, interrupts or spoofs communications between two systems. For example, fake temperature data 'generated' by an environmental monitoring device can be spoofed and forwarded to the cloud. Similarly, an attacker can disable vulnerable heating, ventilation, and air conditioning (HVAC) systems during a heat wave, creating a disastrous scenario for service providers with affected models (rapid7.com/fundamentals/man-in-the-middle-attacks).

4.12.2 Data and Identity Theft

Data generated by unprotected devices and smart appliances provide cyber attackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identify theft by intruders.

4.12.3 Device Hijacking

The attacker hijacks and effectively assumes control of a device. These attacks are quite difficult to detect because the attacker does not change the basic functionality of the device. Moreover, it only takes one device to potentially re-infect all smart devices in the smart daycare center. For example, an attacker who initially compromises a thermostat can theoretically gain access to an entire network and remotely unlock a door or change the keypad PIN code to restrict entry.

4.12.4 Distributed Denial of Service (DDoS)

A denial-of-service attack (DoS attack) attempts to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting

services of a host connected to the Internet. In the case of a distributed denial-of-service attack (DDoS), incoming traffic flooding a target originates from multiple sources, making it difficult to stop the cyber offensive by simply blocking a single source. In fact, DDoS attacks doubled from 3% to 6% in 2016, primarily due to the lack of security in IoT Devices. This isn't surprising, especially as a single compromised smart sensor on a network can infect similar devices running the same software. These infected devices are then forced to join vast botnet armies that execute crippling DDoS attacks.

4.12.5 Permanent Denial of Service (PDoS)

Permanent denial-of-service attacks (PDoS), also known as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. BrickerBot, coded to exploit hard-coded passwords in IoT devices and cause permanent denial of service, is one such example. Another example could see fake data fed to thermostats in an attempt to cause irreparable damage via extreme overheating.

4.13 Security and Privacy Assurance for the Implementation of IoT Based Smart Daycare in Ghana

Connected smart daycare devices will be protected by a comprehensive IoT security solution (device to cloud) that does not disrupt a Service provider or original equipment manufacturer (OEMs) profitability or time to market. A comprehensive IoT security solution will include the following capabilities:

4.13.1. Secure Boot

Secure boot utilizes cryptographic code signing techniques, ensuring that a device only executes code generated by the device OEM or another trusted party. Use of secure boot technology prevents hackers from replacing firmware with malicious versions, thereby preventing attacks which will provide assurance of security and privacy to the users of the system.

4.13.2 Mutual Authentication

Every time a smart daycare device connects to the network it will be authenticated prior to receiving or transmitting data. This ensures that the data originates from a legitimate device and not a fraudulent source. Cryptographic algorithms involving symmetric keys or asymmetric keys can be utilized for two-way authentication. This ensures that the data originates from a legitimate device and not a fraudulent source. For example, the Secure Hash Algorithm (SHA-x) can be used for symmetric keys and the Elliptic Curve Digital Signature Algorithm (ECDSA) for asymmetric keys.

4.13.3 Secure Communication (Encryption)

Protecting data in transit between a device and its service infrastructure (the cloud). Encryption ensures that only those with a secret decryption key can access transmitted data. For example, a smart thermostat that sends usage data to the service operator must be able to protect information from digital eavesdropping.

4.13.4. Security Monitoring and Analysis

Captures data on the overall state of the system, including endpoint devices and connectivity traffic. This data is then analyzed to detect possible security violations or potential system threats. Once detected, a broad range of actions formulated in the context of an overall system security policy will be executed, such as quarantining devices based on anomalous behavior. This monitor- analyze-act cycle may execute in real time or at a later date to identify usage patterns and detect potential attack scenarios. It is critical to ensure that endpoints devices are secured from possible tampering and data manipulation, which could result in the incorrect reporting of events.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Introduction

This chapter presents summary of key findings and draws conclusions on the findings of the research, suggestions and also makes some recommendations. The chapter is put into four sections, section 5.2 gives summary of the findings. Section 5.3 on the other hand gives recommendations for further study and implementation. Section 5.4 draws conclusions on the proposed IOT based smart daycare system and 5.5 provides suggestions for further research.

5.2 Summary of Findings

The key findings from the study reveals that teachers need the IOT smart daycare system to enable them work independently, automate some school processes, improve their ICT competence, monitor student movement and ensure security of kids when effectively used. The study also identified some potential challenges and security threats that affect the system and possible countermeasures to forestall any security possible threats. Such as; network failure, phishing and spoofing attacks, man in the middle attacks and so on. The system when fully implemented ensures significant impact towards improving teaching and learning as revealed by the findings that teachers are more effective in working independently and self-motivated to work at their own pace, teachers develop their knowledge effectively and also help teachers access information and communicate effectively on the progress and security of kids. On the other hand, parents need smart daycare system for child safety and security and the access to information and progress of their kids in school.

This study gathered information concerning the extent of need/effectiveness of the IOT based smart daycare system implementation, some potential security threats associated with its implementation and how the system impacts teaching and learning. It also discusses the principles of IOT smart daycare systems model, how it operates, consistent power supply and potential security threats. The target for this study was teachers and parents of children at Winners Academy daycare, Future Leaders daycare and Mount Zion International daycare all in the Lambussie District.

Security is one of the goals of IoT-based smart daycare but, based on what we have found above (security threats, extend of need/effectiveness and how the system can impact effective teaching and learning) from the results of the study, we see that these technologies are very much vulnerable to different security attacks that make an IoT-based smart daycare a threat and unsecure to live in if security is neglected. Therefore, it is necessary to evaluate, identify and address the security threats, the extend of need and its impact on teaching and learning to judge the situation of the smart daycare. If security in a smart daycare is ignored or if convenience and functionality is preferred over security, there will be adverse implications in terms of its operations.

Smart daycare is a place which is meant to be safe and secure to live in. It must provide sufficient security and privacy assurance. Connecting every smart object inside the daycare to the internet and to each other results in new security and privacy problems, e.g., confidentiality, authenticity, and integrity of data sensed and exchanged by devices.

We can conclude that security is a critical factor and must be taken seriously. That is why there is a proposed intervention as the smart daycare system, a typical smart daycare with the goal of highlighting various security threats in IoT-based smart

daycare, identify issues satisfying most of security requirements and how the system can promote effective teaching and learning in our daycare schools.

In this study, critical information assets were identified on which the security threats were identified with the goal of protecting them. User education is essential to make stakeholders in particular the inhabitants (Teachers) aware of different security threats especially social engineering and the operations of the system.

5.3 Recommendations

Based on the results of the data analyzed in the previous chapter, the study made some key recommendations. Some of the recommendations were to the stakeholders, both the commercial stakeholders (suppliers, infrastructure providers, third party software and hardware vendors etc.) and Non-commercial stakeholders (governmental institutions ie; GES and municipalities/Districts and end-users (inhabitants), with the goal of making improvements in this technology (IoT-based smart daycare), with respect to child security and how its impact on teaching and learning in Ghanaian daycare schools.

These specific recommendations were that;

1. The study recommended that school authorities, parents and Government should implement a sustaining internet and computer training, which will eventually allow Daycare schools to keep pace with developed countries and teachers to be abreast and conversant with system operations.
2. Government/schools should procure adequate ICT facilities to help in the implementation of smart daycare system in Ghana.

3. The Smart daycare schools in Ghana should invest in reliable internet connection in order to make it accessible for Teachers to effectively implement the IOT Smart daycare system.
4. The Daycare institutions should also have alternative source of power in places where there is no electricity so as to enable effective implementation of IOT smart Daycare system.

5.4. Conclusion

The objectives of this study were to propose and develop a secure Internet of Things (IoT) based on the extent of need/effectiveness, identify security threats/challenges and to develop a conceptual model (smart daycare system) for the implementation of IOT based smart daycare system in Ghana to provide intelligence, comfort, improve the quality of life and security of kids as well as promote teaching and learning in schools.

Bringing IoT technology to our school results in new security challenges, therefore IoT-based Smart Daycare require very stringent security requirements. These modern technologies offer both opportunities and risks, an IoT-based Smart Daycare is highly vulnerable to different security threats both from inside and outside the school, if security in a smart daycare or smart device is compromised, the user's privacy, personal information and even safety of the teachers and students will be at risk. Security of the smart daycare and its information assets is critical for child's security and safety. Therefore, appropriate measures have to be taken to make the smart daycare more secure and suitable to live in. But we must know exactly what we are trying to protect and why before selecting specific solutions. A careful assessment of security risks must precede any security implementation to assure that all the relevant, underlying problems are first discovered.

5.5 Suggestions for Further Research

The scope of the current study was limited to only three Daycare educational institutions in Lambussie. This therefore limits the reliability, validity and generalization ability of the study. The study therefore recommends any further study to include other Daycare educational institutions and even expand the sample size. Increase in sample size would help reduce perception biases as well. Also, the list of proposed additional ways in which the same project can be done is provided below:

i. Looking into reasons for adoption of the proposed smart daycare and to check if indeed it can be an intervention to our arising security issues in Ghana.

ii. View the Smart daycare security issues more in depth than this project undertook

iii. The thesis should also include the practical security testing of different Smart daycare to get observation regarding the vulnerabilities.

REFERENCES

Aboderin, O. S., & Kumuyi, G. J. (2013). The problems and prospects of E-learning in curriculum implementation in secondary schools in Ondo state, Nigeria. *International Journal of Educational Research and Technology press, 4*(1), 90–9.

Alheraish, A. (2004). Design and Implementation of Daycare Automation System. China, *IEEE Transactions on Consumer Electronics, 50*(4), 1087-1092.

Ali, U., Nawaz, S. J., & Jawad, N. (2006). A Real-time Control System for Home/Office appliances automation, from mobile device through GPRS network. *In 2006 13th IEEE International Conference on Electronics, Circuits and Systems*, 854-857.

Anene, J. N., Imam, H., & Odumuh, T. (2014). Problem and Prospect E-learning in Nigerian universities. *International Journal of Technology and Inclusive Education (IJTIE), 3*(2), 320–327.

Apthorpe, N., Reisman, D., & Feamster, N. (2017). *A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic*. arXiv preprint arXiv:1705.06805.

Ashton, K. (2009). That 'Internet of things' thing. RFID journal

Atukorala, K., Wijekoon, D., Tharugasini, M., Perera, I., & Silva, C. (2009). SmartEye Integrated solution to Daycare Automation, security, and monitoring through mobile phones. *Third International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST '09*, 64-6.

Azitiria, A., & Izaguirre, A. (2008). *Autonomous Learning of User's Preferences Improved through user feedback*. United Kingdom: Mondragon University, Research Gate.

Bellotti, V., & Edwards, K. (2001). Intelligibility and accountability: Human considerations in context-aware systems. *Human–Computer Interaction, 16*(24), 193-212.

Bryman, A. (2012). *Social research method*. Oxford: Oxford University Press.

Chahuara P., Fleury A., Portet F., & Vacher M. (2012). *Using Markov Logic Network for On-Line Activity Recognition from Non-visual Daycare Automation Sensors*. In: Paternò F., de Ruyter B., Markopoulos P., Santoro C., van Loenen E., Luyten K. (eds) Ambient Intelligence. Lecture Notes in Computer Science, 7683. Berlin, Heidelberg: Springer.

Choi, J., Shin, D., & Shin, D. (2005). Research and implementation of the context-aware middleware for controlling home appliances. *IEEE Transactions on Consumer Electronics, 51*(1), 301-306.

Cohen, L., Manion, L., & Morrison, K. (2011). *Research methods in education: Creative Education*.

Creswell, J., & Plano, C. (2011). Designing and Conducting Mixed Methods Research. *Open Journal of Nursing, 6*, 12-24.

Danaher, M., & D. Nguyen, (2002). Mobile Home Security with GPRS, in proceedings of the 8th International Symposium for Information Science.

Dawadi, P. N., Cook D. J., & Schmitter-Edgecombe, M. (2016). Automated Cognitive Health Assessment from Smart Daycare-Based Behavior Data. *In IEEE Journal of Biomedical and Health Informatics, 20*(4), 1188-1194.

Delgado, A. R., Picking, R., & Grout, V. (2009). *Remote-controlled daycare automation systems with different network technologies.* Wales: Centre for Applied Internet Research (CAIR), University of Wales.

DeVaus, D. A. (2002). *Surveys in social science research* (5th ed.). London: Routledge.

Dey, A. K. (2001). Understanding and using context. *Personal and ubiquitous computing, 5*(1), 4-7.

Dich, N., & Pedersen, B. (2013). Native Language Effects on Spelling in English As a Foreign Language. *Canadian Journal of Applied Linguistics, 33*, 101-115.

Doctor, F., Hagras, H. A., & Callaghan, V. (2012). An intelligent fuzzy agent approach for realising ambient intelligence in intelligent inhabited environments. *IEEE Transition System Manufacturer Cyber, Part A: System Humans, 35*(1), 55–65.

Eckersley, P. (2010). How Unique Is Your Browser? Proceedings of 10th Privacy Enhancing Technologies Symposium (PETS), Berlin, Germany.

Eze, C. S., Chinedu-Eze, C. V., & Bello, O. A. (2018). The utilisation of e-learning facilities in the educational delivery system of Nigeria: A study of M-University. *International Journal of Educational Technology in Higher Education, 2*(8), 15-34.

Fleury, A., Vacher, M., & Noury, N. (2010). SVM-based multimodal classification of activities of daily living in health smart daycares: Sensors, algorithms, and first experimental results. *IEEE Transition Information Technology Biomedical, 14*(2), 274–283.

Flick, U. (2011). *Introducing Research Methodology: A Beginner's Guide to Doing a Research Project*.

Gentles, S. (2015). *Sampling in Qualitative Research*.

Guest, G., Namey, E., & Mitchell, M. (2013). *Collecting Qualitative Data: A field manual for applied* res Yang, K. T., Ni, C. C., Teng, W. C., Hsiang T. R., & Lee Y. J., (2012) Clock skew-based client device identification in cloud Environments. in AINA, L. Barolli, T. Enokido, F. Xhafa, and M. Takizawa, Eds. IEEE, 526–533.

Hammond, M., & Wellington, J. (2012). *Research Methods: The Key Concepts*.

Heale, R., & Twycross, A. (2015). *Validity and reliability in quantitative studies. Evidence based nursing*.

Huang, P. H., Su, J. Y. Z., Lu, M. J., & Pan, S. (2016). A fire-alarming method based on video processing. *Intelligent Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 359-364.

Intille, S. S. (2002). Designing a home of the future. *IEEE Pervasive Computing, 1*(2), 76-82.

Jin, J., Jing J., Wang, Y, Zhao., K., & Hu, J. (2008). Development of Remote-Controlled Daycare Automation system with Wireless Sensor Network. *Fifth IEEE International Symposium on Embedded Computing, SEC '08*, 169-173.

Jose, V. D., & Vigyakshmi, A. (2018). *An overview of security in IOT*. 8th International Conference on Advances in Computing and Communication (ICACC-2018). Open access, Elsevier publications.

Kanma, H., Wakabayashi, N., Kanazawa, R., & Ito, H. (2003). Home appliance control system over Bluetooth with a cellular phone. *IEEE Transactions on Consumer Electronics, 49*(4), 1049-1053.

Kasteren, T. L. M., Englebienne, G., & Kröse, B. J. A. (2009). An activity monitoring system for elderly care using generative and discriminative models. *Personal and Ubiquitous Computing*, 1–9.

Kelion, L. (2014). *Breached webcam and baby monitor site flagged by watchdogs*, http://www.bbc.com/news/technology-30121159, BBC News,

Khiyal, M. S. H., Khan, A., & Shehzadi, E. (2009). SMS based wireless home appliance control system (HACS) for automating appliances and security. *Issues in Informing Science & Information Technology, 6,* 31.

Kimberlin, C., & Winterstein, A. (2008). Validity and Reliability of Measurements used in Research . *American Journal of Health*.

Kirsh, D. (2002), "E-learning, metacognition and visual design", paper presented at the International Conference on Advances in Infrastructure for e-Business, e-Education, e-Science, and e- Medicine on the internet, 3, 213-333.

Konidala, D. M. Kim, D. Y. Yeun, C. Y. & Lee, B. C. (2011). Security framework for RFID-based applications in smart daycare environment. *Journal of Information Processing Systems, 7*(1), 111–120.

Kumar. S., Tiwari. P., & Zymbler. M., (2019). Internet of things is a revolutionary approach for future technology enhancement: A review journal of big data-springer, department of information engineering, University of Padova, Itally, Podua pree

Leavy, P. (2017). *Research design: Quantitative, qualitative, mixed methods, arts based, and community based participatory research approaches*. Guilford Press.

Luotonen, A. (1994). World-wide web proxies. *Computer Networks and ISDN systems, 27*(2), 147-154.

Madakam, S., Ramasmami, R., & Tripathi, S. (2015). Internet of things (IOT): A literature review, open access, Vol.03 No. 05 (2015), Article ID:56616,10 pages

10.4236/jcc.2015.35021

Maekawa, T., Kishino, Y., Sakurai, Y. & Suyama, T. (2013). Activity recognition with hand-worn magnetic sensors. *Pers. Ubiquitous Compute, 17*(6), 1085–1094.

Manir, A. K. (2007). The Internet as tool for Interactive Learning, Teaching and Research. *International Journal of Emerging Technologies in Learning, 2*(3), 34-53.

Mayer, J. R. (2009). Any person... a pamphleteer: Internet Anonymity in the Age of Web 2.0‖, Undergraduate Senior Thesis Submitted in partial fulfilment of the Requirements of Princeton University for the B.A Degree. Princeton, New Jersey, USA: Princeton University.

Mbarek, R., & Zaddem, F. (2013). The examination of factors affecting e-learning effectiveness. *International Journal of Innovation and Applied Studies*.

Merilahti, J., Pärkkä, J. Antila, K., Paavilainen, Mattila, P. E., Malm, E. J., Saarinen, A., & Korhonen, I. (2009). Compliance and technical feasibility of long-term health monitoring with wearable and ambient technologies. *J. Telemed. Telecare, 15*(6), 302–309.

Mihailidis, A., Carmichael, B., & Boger, J. (2004). The use of computer vision in an intelligent environment to support aging-in-place, safety, and independence in the home. *IEEE Trans. Inf. Technol. Biomed., 8*(3), 238–247.

Mokhtari., G., Zhang, Q., Nourbakhsh, G. B., & Stephen., K. M. (2017). BLUESOUND*:* A New Resident Identification Sensor-Using

Ultrasound Array and BLE Technology for Smart Home Platform. IEEE Sensors Journal, 17(5), 1503-1512.

Monekosso, D. N., & Remagnino P., (2010). "Behavior Analysis for Assisted Living," in *IEEE Transactions on Automation Science and Engineering, 7*(4), 879-886.

Montrieux, H., Vanderlinde, R., Schellens, T., & De Marez, L. (2015). *Teaching and Learning with Mobile Technology: A Qualitative Explorative Study about the Introduction of Tablet Devices in Secondary Education*.

Morsalin, S., Islam, A. M. J. Rahat, G. R., S. Pidim, R. H., Rahman, A. & M. Siddiqe, A. B. (2016). "Machine-to-machine communication based smart daycare security system by NFC, fingerprint, and PIR sensor with mobile android application," 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), Dhaka, Bangladesh, 2016, pp. 1-6.

Mowery, K. & Shacham, H. (2012). Pixel perfect: Fingerprinting canvas in HTML5‖, Proceedings of W2SP 2012, M. Fredrikson, Ed. IEEE Computer Society.

Nakibly, G., Shelef, G., & Yudilevich, S. (2015). "Hardware Fingerprinting Using HTML5", Cornell University Library (CoRR), abs/1503.01408.

Nivedha, K., Anitha, K., Jayaprakash, D., & Sathish, K.R(2020). Design and implementation of smart daycare monitoring system. European journal of molecular and chemical medicine, India, TamilNadu press.

Oppong, S. H. (2013). The problem of Sampling in Qualitative Research, Asian Journal of Management Sciences and Education, Vol. 2, No. 2.

Paavilainen, P., Korhonen, L¨otj¨onen I. J., Cluitmans, L., Jylh¨a, M., S¨arel¨a, A. and Partinen, M. (2005). “Circadian activity rhythm in demented and non-

demented nursing-home residents measured by telemetric actigraphy," J. Sleep Res., vol. 14, no. 1, pp. 61–68, Mar. 2005.

Richard, & Haya. (2009). factors influencing the adoption of the elearning technology in teaching and learning. European Scientific Journal.

Robertson, G. M.T. (2000), "Perceptual user interfaces", Communications of the ACM, 43(2), 53-68.

Saeed, U., Syed, S., Qazi, S. Z., Khan, N., Khan, A., & M. Babar, (2010). Multi-advantage and security-based Daycare Automation system. Fourth UKSim European Symposium on Computer Modeling and Simulation (EMS), 7-11.

Saponara, S., & Bacchillone, T. (2012). Network architecture, security issues, and hardware implementation of a home area network for smart grid. *Journal of Computer Networks and Communication, 20*, 534512-534512.

Saris, W., & Gallhofer, I. (2014). *Design, Evaluation and Analysis of Questionnaires for Survey Research*. New York.

Sulley, S. Y. (2019). Kidnapping in Ghana: An emerging crisis. Ghana, UDS press

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Studies*. Pearson; 6 edition.

Schilit, B. N., & Theimer, M. M. (1994). Disseminating Active Mop Infonncition to Mobile Hosts. IEEE network.

Sekaran, U., & Bougie, R. (2010). Research Methods for Business.

Sreejesh, S., & Mohapatra, S. (2014). Mixed Method Research Design.

Sriskanthan, N., Tan, F., & Karande, A. (2002). "Bluetooth based Daycare Automation system," Microprocessors and Microsystems, Elsevier, vol. 26, pp. 281-289.

Subhash, N. (2018). Cambridge Montessori global, Aggarwal Millennium Tower 1, Jalsa Ventures Group Company, Deli 110034.

Tapia, E. M., Intille S., S., & Larson K. (2004). Activity Recognition in the Home Using Simple and Ubiquitous Sensors. In: Ferscha A., Mattern F. (eds) Pervasive Computing. Pervasive 2004. Lecture Notes in Computer Science, vol. 3001. Springer, Berlin, Heidelberg.

Tlaitlai, M.M., Makurunge, T., & Bhila, T. (2021). Green design as a model for healthy daycare centers in Lesotho: "An enhancing and nurturing environment for children". Research gate. Lesotho, Limkokwing university of creative technology press.

Van Laerhoven K., Kilian, D., & Schiele, B. (2008). "Using rhythm awareness in long-term activity recognition," in Proc. IEEE Int. Symp. Wearable Computers, pp. 63–66.

Wannenburg, J. & Malekian, R. (2016). "Physical Activity Recognition from Smartphone Accelerometer Data for User Context Awareness Sensing," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. PP, no.99, pp.1-8.

Wu, B., Peng H., & Chen C. (2006). "A Practical Home Security System via Mobile Phones," TELE-INFO'06 Proceedings of the 5th WSEAS international conference on Telecommunications and informatics, pp. 299-304.

Yang, L., Yang, S. H., & Yao, F. (2006). Safety and security of remote monitoring and control of intelligent home environments. In Systems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on (Vol. 2, pp. 1149-1153). IEEE.

Yürür, Ö., Liu, C. H., Sheng, Z., Leung, V. C., Moreno, W., & Leung, K. K. (2014). Context-awareness for mobile sensing: A survey and future directions. *IEEE Communications Surveys & Tutorials, 18*(1), 68-93.

Zander, S., & Murdoch, S. J. (2008). An improved clock-skew measurement technique for revealing hidden services. In: 17th conference on Security symposium (SS '08), July 28 - August 01 2008, San Jose, CA.

Zheng, H., Wang, H., & Black, N. (2008). International Conference on Networking, Sensing and Control - Human Activity Detection in Smart Home Environment with Self-Adaptive Neural Networks, (), IEEE 1505–1510.

Zohrabi, M. (2013). *Mixed Method Research: Instruments, Validity, Reliability and Reporting Findings*

Zuo, F., & De With, P. H. (2005). Real-time embedded face recognition for smart daycare. *Consumer Electronics, IEEE Transactions on, 51*(1), 183-190.

APPENDIX A

UNIVERSITY OF EDUCATION, WINNEBA

COLLEGE OF TECHNOLOGY EDUCATION, KUMASI

SCHOOL OF GRADUATE STUDIES

QUESTIONNAIRE FOR TEACHERS AND PARENTS

Dear respondents,

Directions: Please answer each question as accurately as possible by ticking (√) and circling the appropriate column to the right of the option. All information gathered is purely for research purposes and shall be treated confidential. Thanks.

SECTION A: RESPONDENTS' BIO-DATA

1. Please indicate your gender.
   [ ] male [ ] female

2. Please what is your age group?
   [ ] below 30 years [ ] 30 – 35 years [ ] 36 – 40 years
   [ ] 41 – 45 years [ ] above 45yrs

3. What is your marital status?
   [ ] married [ ] single (not married) [ ] other……

Section B: Extent of need of IOT based smart daycare system implementation in daycare environment.

4. Indicate to what extent do you need an IOT based smart daycare system, (using a scale of 1 – Large Extent, 2- Some Extent, 3- Undecided, 4 – Less Extent, 5 No Extent). **Please tick the box which best reflect your view and state briefly where necessary**

S/N	Statements	Scale				
		1	2	3	4	5
	Smart daycare system for working independently and self-directed					
1.	Teachers need system to adjust to its usage					
2.	Teachers need alarm system component to organize students					
3.	Teachers need the system to work independently through sensors					
4.	Teachers are not ICT literate and may find it difficult to adjust to system usage.					
	Smart daycare model for safety of kids and school					
1.	Teachers need the system to monitor student movement					
2.	Teachers need the system to protect school property					
3.	Teachers need the system to prevent unlawful intruders					
	Smart daycare system for learning and understanding					
1.	Classroom contain interactive smart devices to enhance learning					
2.	Teachers need the system to introduce more technology tools to kids					
3.	Most Teachers need adequate knowledge in the use of the system devices when implemented					

	Smart daycare system for contact out of class					
1.	Teachers need the system to check register of attendance					
2.	Teachers need the system to regularly communicate with parents					
3.	Teachers need the system to work collaboratively with their colleagues and parents					

Section C: Challenges and security threats associated with the use of IOT based smart daycare system architecture.

4. To what extent do you agree or disagree with the following statement about the challenges associated with the use of IOT based smart daycare system architecture. Please rate your responses using a scale of 1 to 5: Strongly disagree (1), Disagree (2), Neutral (3), Agree (4), and strongly agree (5). **Please tick the box which best reflect your view and state briefly where necessary**

S/N	**Statements**	**Scale**				
		1	**2**	**3**	**4**	**5**
1.	Lack of basic and adequate infrastructure/ resources					
2.	Lack of IT technicians and personnel					
3.	Insufficient funds to upgrade and maintain the equipment and facilities					
4.	Interruption of system by electricity					
5.	Computer network failure during communication					
6.	Attacks from hackers and predators to gain access to unauthorized information.					
7.	Antivirus and spyware threats on the system resources					
8.	Phishing and spoofing attacks on system data and					

	resources					
9.	Lukewarm attitudes of some parents concerning child welfare and safety					
10.	Inadequate knowledge on how to use and operate the system					
11.	A breakdown in the system exposes children to risk					

Section B: Effectiveness of smart daycare system implementation by teachers

4. To what extent do you agree or disagree with the following statement about effectiveness of smart daycare system use by teachers. Please rate your responses using a scale of 1 to 5: Strongly disagree (1), Disagree (2), Neutral (3), Agree (4), and strongly agree (5). **Please tick the box which best reflect your view and state briefly where necessary**

S/N	**Statements**	**Scale**				
		1	**2**	**3**	**4**	**5**
	Effective in working independently and self-motivated					
1.	Teachers are more effective in using the system to monitor kids					
2.	Teachers are more effective in controlling student movement on campus					
3.	Teachers are more effective submitting work on time					
4.	Teachers are more effective organizing their work					
5	Teachers are more effective in training students to use smart devices for learning.					
6	Teachers are more effective working independently					
	Teachers to develop knowledge effectively					
1.	Teachers are more effective developing their understanding on system operation.					

2.	Teachers are more effective reinforcing their knowledge					
3	Teachers are more effective engaging with the kids in class					
4.	Teachers are more effective managing students using the system after school					
	Access information and communicate effectively					
1.	Teachers are more effective using GSM/mobile based daycare automation for communication.					
2.	Teachers are more effective contacting parents of kids					
3.	Teachers are more effective monitoring students from outside class					
4.	Teachers effectively have peace of mind to interact with kids					
5.	Teachers are more effective in using the CCTV cameras.					
	Research and present information effectively					
1.	Teachers are more effective presenting assessment results of kids electronically					
2.	Teachers are more effective in using internet-based daycare system for communication					
3.	Teachers and kids are more effective researching topics					

Thank you