World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

An enhanced Framework for Implementing Secure Wireless Network

Odero James Kenneth * and Abeka Silvance

Jaramogi Oginga Odinga University of Science and Technology, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(03), 260-274

Publication history: Received on 03 May 2026; revised on 16 June 2026; accepted on 19 June 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.3.0314

Abstract

With the rapid evolving of the digital threat landscape sophisticated attacks are being launched with malicious actors daily. Security frameworks such as COBIT 5 and ISO 27001 have been there for some since the earlier days of the internet hence they have evolved to support new technologies and defend against new threats. However there have been concern about the effectiveness of the security frameworks in regards to safeguarding the wireless networks against recent threats. Security frameworks such COBIT 5 and ISO 27001 variables cannot be mapped one to one into the administrative, Technical, Physical and monitoring and evaluations security controls. Moreover they are not role based. This paper presents an enhanced security framework which can be used to secure wireless networks and it is role-based meaning that organizations can simply assign responsibilities to employees based on it. The study adopted quantitative research design in which target population of the study was of 296 staff. Purposive, stratified and simple random sampling techniques were used to select the participants. Structured online questionnaires using google forms was used to collect data from a sample of 148 respondents. Multiple regression analysis was used to examine the effect of security controls on secure wireless network. From the results security controls influenced secure wireless network. The study recommends the implementation of an enhanced security framework to organizations using wireless network in order to safe guard their networks.

Keywords: Attacks; Security Frameworks; Security Controls; Threats; Wireless Network

1. Introduction

Wireless networks (WNs) is expanding in sky rocketing speed as it continues to be adopted globally due its advantages feature over cable network such as lack of writing, scalability, ease of installation, mobility, flexibility and reducing prices of the wireless devices. Its usage is fast growing in smart applications such smart cities, intelligent traffic management, e –health, smart agriculture and smart grids. Hence making wireless networks to be part of our daily activities [1,2,3,4].

Over the years, wireless networks have grown exponentially due to the proliferation of computing devices such smartphones, tablets and laptops and continues development of the radio technologies. Ever since the introduction of wireless technology, security has been a vital issue hence the technology suffers from serious security attacks and vulnerabilities. Several papers have been presented on security attacks in wireless network [14, 15]. According to [12, 13] attacks can be classified into two as active and passive attacks. In active attacks the attacker's motive is to modify, alter or harm the network and the attack target the availability and integrity of the network services. Passive attacks the attacker target is to eavesdrop and sniff the information in order to have an overview about the network. In passive attack the attacker does not modify or alter the data flowing across the network hence he only collects information in which he can use to attack and harm the wireless network. Active attacks are denial of service, rogue access point, spoofing and man-in-the middle attacks while passive attacks are traffic analysis and eavesdropping. The security risk of the authorized access point is that it could be used to steal or leak sensitive information such passwords, bio data,

* Corresponding author: Odero James Kenneth

employee's records in an organization [26, 27, 28]. According to [33, 34], traffic analysis attack occurs when an attacker analyzes the pattern of wireless communication channel that later discloses the pattern to an intruder to harm the wireless network. MITM attack is a common attack in both wired and wireless networks. It occurs when an attacker intercepts the communications between two parties in network without the knowledge of the two parties. The attacker (the man in middle) may use attack to steal, modify, or disrupt the communication between the two parties [16, 17, 18].

Moreover, weak authentication protocols such as Wired Equivalent privacy (WEP) which is easily too compromised due to the vulnerability of the static key which can be effortlessly be intercepted and utilized hence it not recommended in utilizing WEP nowadays [38, 39, 40, 41]. In addition, the concept BYOD where it has become trend of employees of an organization to use their personal devices to connect to their organization networks, access work related systems and confidential data thus it creates security vulnerability to wireless network. The personnel devices could be used as platform to engineer attacks in the wireless network. Hence it is prudent for an organization to have well prepared BYOD policy to assist to improve the security of wireless network [42, 43, 44, 45]. Finally, the wireless medium which has been topic of discussion for quite some time due the open nature of it makes it very vulnerable all sorts of attacks such as jamming and scrambling of the wireless signals [46, 47, 48]. Hence, authentication and key management could the solution deal with various attacks in the wireless environment [49,50].

Security frameworks refers to a collection of standards, policies, procedures and best practices that are well documented with the aim to manage risk and minimize vulnerabilities. It can also be used to assist in preparing for compliance and other IT audits. Security frameworks have been there for some time since the earlier days of the internet hence they have evolved to support new technologies and defend against new threats. The study looks at HIPAA, PCI-DSS, COBIT 5, ISO / IEC 27001 and NIST Cybersecurity Frameworks.

Security controls are parameters implemented to reduce or mitigate the risk associated with organization assets. Any kind of mitigation or counter measure used to detect, counteract, avoid or reduce security risk to people, property and data is considered as security control [60,61]. It is very important for every organization to access the risk associated with wireless network in order to select the appropriate security control to implement [62.63].

1.1. Statement of the Problem

Although the benefits of wireless networks are substantial, the technology poses great security and privacy concerns due the openness of the wireless communication channel where data transmitted over channel could easily be eavesdropped or tampered with by intruders. Hence, it is crucial to safeguard data and provide privacy protection in WLANs. Moreover, strong security solution and authentication protocols are required for the success and widely deployment of wireless network [64].

In recent years, various researchers have proposed several authentication protocols based on different mechanisms and security frameworks as means to ensure data confidentiality, integrity and availability in wireless network. However most these protocols and framework security cannot cope with common attacks such as man-in –the middle (MITM) attacks, impersonation attacks and device capture attacks [65].

In [8], the authors who carried out a study to investigate security threats associated with wireless networks in Kenya universities found out that many institutions of higher learning are not aware of the specific risk they face while using their networks. Some lack the network monitoring mechanisms while many do not conduct security assessment hence they cannot identify corrective measures and actions. Generally, the study unearths that wireless networks deployed in most institutions of higher learning in Kenya is not secure though efforts have been put by different institutions to ensure secure network thus efforts are not comprehensive. Data transmitted via wireless networks mostly take place over public channels which are prone to attacks, eavesdropping and modification of information over the channel hence secure authentication protocol is enviable in order to safe guard the wireless network [9,10,11]. It is thus evident the security of wireless network is wanting hence this research seeks to come up with enhanced security framework that will effectively and efficiently safe guard the wireless network against the attacks.

1.2. Study Objective

This research aims to:

- Develop an enhanced security framework for Wireless Local Area Networks.
- Validate the developed security framework.

2. Literature Review

2.1. Review of Frameworks for WLAN security

Health Insurance Portability and Accountability Act (HIPAA) was established to address the insurance coverage for workers who switch or leave jobs. It is now best known for protecting the privacy of health information by regulating it use and disclosure by entities involved. These entities include clearing houses, healthcare providers and sponsors. Moreover, it ensures that all Protected Health Information (PHI) are safe guarded and access to health data is restricted to authorized personnel only hence, safe guarding health frauds [66]. However, HIPAA as complex compliance requirement with require significant resources and expertise for compliance hence diverting time and resources further away from patients. The administrative chores associated with HIPAA compliance are documentation, training and verifications which is time-consuming and draws away focus from patient care. Moreover, HIPAA's strict privacy regulation can create barricades to effective data sharing among health providers leading to disintegrated care and lack for comprehensive treatment. In addition, legal consequences of HIPAA violation can create fear and anxiety among healthcare professionals leading to potential defensive approach to patient care [66, 67, 68].

The Payment Card Industry Data Security Standard (PCI -DSS) is a framework for institutions that handle payment cards. It is global standard for all organizations that store, process or transmit cardholder data. It sets baseline level of safe guarding for consumers and assist to minimize fraud and data breaches in the payment ecosystem. Moreover, it acts baseline of other compliance frameworks. It is used by organizations that process payment cards [69]. However, this framework is mandatory for business or organization dealing with payment cards hence noncompliance lead to fines, penalties and bad reputation of the business. The framework is very technical that require expertise to understand so that they implement it in the right way. In addition to ensure a third-party service provider follow the regulation is very difficult and they are competency gaps on understanding requirements among organizations.

COBIT is a management and governance framework that assist organizations maintain an ideal balance risks, benefits and resource utilization. COBIT 5 is based on five principles that are critical for management and governance of enterprise IT which are meeting stakeholder needs, covering the enterprise end to end, applying a single integrated framework and separating governance from management. The framework enhances decision making process and optimizes the business process by bridging gap IT and business alignment [70]. However, many organizations avoid to implement COBIT 5 is considered to be complex since it brings in the IT management and Enterprise governance all in one outfit. Furthermore, it requires a lot of skills and knowledge to be used as tool to offer IT governance support or assess the performance of IT department in an organization. Moreover, it shows how to achieve good governance criteria but does not provide details of the implementation of good IT governance. COBIT 5 is usually popular used for audits, where audit is usually places at the end of the activities as a mirror and evaluation of activities that are already running. Since audits are not done frequently, usually done every 6 months or once year thus conclusion can be drawn that COBIT 5 is hardly used as daily operational standard. Lastly it resources intensive to implement mainly for small organizations [71, 72].

ISO/IEC 27001 is a global standard for data security that was setup by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC.) It provides assists for creating an information security management system (ISMS) which covers is people, process and technology. It provides a framework that institutions can use to safeguard their assets by use of various technologies, auditing practice and tests. It is central standard explaining best practice for information security management and it used to audit and certify organizations [73, 74, 75]. The framework covers wide range of controls related to information security and the Plan-Do-Check-Act (PDCA) cycle is the heart of the framework which encourages continuous improvement for organizations. Despite ISO 27001 being known to be standard for information security management systems its faces with the following limitations. The standard's comprehensive and technical language can be complex and difficult for organizations especially those that do have experience in information security management. The complexity may lead to misinterpretations of the requirements. The ISO 27001 furnishes a structured framework in which some institutions may find it rigid for specific tasks. Following the standard requirement strictly may not always align with unique cultures or operational activities of some organizations. The standard provides with general guidance on information security management misses industry-specific requirements thus organizations may require to supplement ISO 27001 with another standard or best practices to tackle specific industry. Lastly getting ISO 27001 certification requires rigorous audit processes and assessment to be conducted by authorized certification bodies in which some organization may fail to comply with [76, 77, 78].

NIST Cyber Security Framework is a set of best practices, standards and recommendations that assist institutions to enhance their cyber security measures. The standard was compiled by NIST after former United States president Baraka

Obama signed an executive order to establish a set of voluntary cyber security standard for critical infrastructure [79]. The framework enables long-term cyber security and risk management. It is designed to meet future compliance and regulation requirements hence it conciliate the interest of business and technical shareholders. NIST Cyber Security Framework has evolved ever since it was introduced in 2014 however the framework has the following limitations with its approach to cyber security. Due to the fact cyber security expertise are few which lead to scarce resource in the industry. There is need to automate some of the implementation steps of this framework which is lacking. Moreover, it shows directional improvement but cannot show the Return on Investment (ROI) of improvement and does not have any formal certificate of compliance. There is need for organizations to consider additional framework or approaches to complement NIST Cyber security framework in order to enhance their risk management practices [80]

Thus, there are various cyber security frameworks such as ISO 27000 series, COBIT 5, PCI-DSS, NIST cyber security framework however no single framework will fully safeguard an organization against threats and attacks since each framework has its advantages and disadvantages. However, an organization could use hybrid framework by selecting specific controls from other frameworks to align the business objectives and the compliance requirements. This approach enables flexibility when the technology and threat landscape changes. Therefore, this study selected controls from ISO and NIST frameworks with specific focus on administrative, technical, physical controls and monitoring and evaluation.

3. Methodology

The study adopted quantitative research design in which numerical data was collected among ICT staff of Public Universities in Kenya. The study targeted 249 ICT staff out of which a sample of 148 was used. According to [81] at least 30% of the target population is adequate as the sample size. The study focused on 50 % of the target population as the sample size. This research employed three sampling methods which are purposive, stratified and simple random sampling methods. Purposive sampling was used to select the twenty public universities which have good network infrastructure that support wireless network and has been improving over time. Random sampling was used to select ICT personnel of each strata (public university) so that each person gets equal chance to be chosen.

Table 1 Number of target respondent

Universities	Target population	Sample selected (50%)
U1	25	13
U2	10	5
U3	22	11
U4	18	9
U5	20	10
U6	15	8
U7	20	10
U8	15	5
U9	14	8
U10	11	6
U11	15	8
U12	11	6
U13	13	7
U14	12	6
U15	10	5
U16	24	12
U17	10	5

U18	10	5
U19	8	4
U20	12	6
Total	295	148

The study used online questionnaires using google forms to collect data from the respondents. Reliability was tested and a Cronbach's Alpha value of 0.82 was obtained. Validity was tested using content validity whereby the instruments of data collection was examined by experts in the ICT field to ensure that questions were clear in terms of content, language and implied meaning before being given out to participants. In this research analysis, completed questionnaire responses were edited for completeness, consistency, accuracy and viability before they are tabulated and coded. Further inferential statistics was also utilized whereby regression analysis was conducted. Regression analysis was done to establish the effect of security controls on secure wireless network. The regression model used was as follows:

$$Y=B_o+B_1X_1+B_2X_2+B_3X_3+B_4X_4+B_5X_5+B_6X_6+B_7X_7+B_8X_8+B_9X_9+B_{10}X_{10}+B_{11}X_{11}+B_{12}X_{12}+B_{13}X_{13}+B_{14}X_{14}+B_{15}X_{15}+\varepsilon$$

Where
Y=Secure wireless network
Bo=Constant
X_1= BYOD policy
X_2 = Incident Response Plan
X_3= Principle of Least Privileges (POLP)
X_4 = Password Management Policies
X_5 = Firewall
X_6= Antivirus Software
X_7 = Intrusion Detection System/ Intrusion Prevention System
X_8= Authentication Protocol
X_9 = CCTV Cameras
X_{10}= Security Guard
X_{11}= Proper Fencing
X_{12}=Biometric Technology
X_{13}= Auditing
X_{14}= Continuous Training
X_{15}= Review of Security policies
ε = Error term

4. Results and discussion

4.1. Questionnaire Responses Rate

The link to the online questionnaire was sent via email and WhatsApp to 148 respondents of the selected public universities. Out of the 148 respondents targeted, 131 completed the questionnaire. This represented a response rate of 88.5%.

Table 2 Response Rate

Response	**Frequency**	**Percentage**
Filled in Questionnaires	131	88.5%
Un-returned Questionnaires	17	11.5%
Total response rate	148	100%

The response rate was within the recommendation of 50% which adequate for carrying out analysis and making proper conclusions for the study [82].

4.2. Regression Analysis Results

Regression results on the effect of security controls on secure wireless network of public Universities in Kenya shown in the table below:

Table 3 Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate	Change Statistics				
					R^2 Change	F Change	df1	df2	Sig. F Change
1	.839[a]	.704	.666	.548	.704	18.263	15	115	.000
Predictors: (Constant), review of security policies, Continuous training, Principle of Least Privileges, Incident response plan, CCTV cameras, Security guard, Authentication protocol, Password management Policies, Proper fencing, Firewall security, BYOD policy to boost security, Biometric technology, Auditing of the network, Intrusion detection system & intrusion protection system, Antivirus software.									

According to the model summary Table 3, the fifteen variables that were studied explains 70.4% of variance in secure wireless network as represented by the R^2 while other factors not covered by the study contribute to 29.6% of secure wireless network.

Table 4 ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	82.261	15	5.484	18.263	.000[b]
	Residual	34.533	115	.300		
	Total	116.794	130			
a. Dependent Variable: An enhanced security framework can boost secure wireless network.						

ANOVA (Analysis of variance) was used to determine whether there was a regression relationship between the variables studied. Table 4 revealed that the model can be used to explain the effect of security controls on secure wireless network as P=0.000 which is significant. This indicates that the model is feasible and can be used to predict the effect of the independent variable on the dependent variable.

Table 5 Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	**-.818**	**.403**		**-2.030**	**.045**
BYOD Policy	.127	.060	.131	2.125	.036
Incident response plan	.024	.042	.030	.563	.574
Principle of Least Privileges	.014	.050	.016	.288	.774
Password management Policies	.182	.047	.217	3.838	.000
Firewall	.106	.043	.141	2.444	.016
Antivirus software	.172	.073	.162	2.364	.020
Intrusion detection system & intrusion protection system	.149	.055	.179	2.700	.008
Authentication protocol	-.013	.103	-.007	-.123	.902

	CCTV cameras	.119	.056	.112	2.132	.035
	Security guard	.068	.044	.083	1.526	.130
	Proper fencing	-.029	.056	-.029	-.515	.608
	Biometric technology	.102	.049	.128	2.082	.040
	Auditing	.102	.048	.136	2.116	.036
	Continuous training	.162	.066	.172	2.439	.016
	review of security policies	-.027	.044	-.034	-.615	.540
Dependent Variable: An enhanced security framework can boost secure wireless network						

The regression model;

$Y=B_o+B_1x_1+B_2x_2+B_3x_3+B_4x_4+B_5x_5+B_6x_6+B_7x_7+B_8x_8+B_9x_9+B_{10}x_{10}+B_{11}x_{11}+B_{12}x_{12}+B_{13}x_{13}+B_{14}x_{14}+B_{15}x_{15}$

Therefore, it becomes;

$Y=-0.818+0.127x_1+0.024x_2+.014x_3+0.182x_4+0.106x_5+0.172x_6+0.149x_7-0.013x_8+0.119x_9+.068x_{10}-.029x_{11}+.102x_{12}+.102x_{13}+.162x_{14}-.027x_{15}$

However, from table 5, **"Sig."** column indicates statistical significance of the regression model that was obtained. As rule of thumb that if the P-Values are less than the significance level (usually 0.05) then the regression model is statistically significant to predict the outcome variable. From table 4.12, only nine variables out the fifteen variables are statistically significant hence the regression model will be:

$Y=-0.818+0.127x_1+0.182x_2+0.106x_3+0.172x_4+0.149x_5+0.119x_6+0.102x_7+0.102x_8+0.162x_9$

X_1 = BYOD Policy

X_2= Password Management Policies

X_3= Firewall

X_4= Antivirus software

X_5= Intrusion detection system & intrusion protection system

X_6= CCTV cameras

X_7= Biometric technology

X8= Auditing

X_9= Continuous training

Assuming that all other independent variables are constant secure wireless network will be -0.818. A unit increase in BYOD policy to boost security leads to 0.127 increase in secure wireless network and it is statistically significant at 0.036. A unit increase in Password management Policies leads to 0.182 increase in secure wireless network and it is statistically significant at 0.000. A unit increase in Firewall security leads to 0.106 increase in secure wireless network and it is statistically significant at 0.016.A unit increase in Antivirus software leads to 0.172 increase in secure wireless network and it is statistically significant at 0.020. A unit increase in Intrusion detection system & intrusion protection system leads to 0.149 increase in secure wireless network and it is statistically significant at 0.008. A unit increase in CCTV cameras leads to 0.119 increase in secure wireless network and it is statistically significant at 0.035. A unit increase in Biometric technology leads to 0.102 increase in secure wireless network and it is statistically significant at 0.040. A unit increase in Auditing of the network leads to 0.102 increase in secure wireless network and it is statistically significant at 0.036. A unit increase in continuous training leads to 0.162 increase in secure wireless network and it is

statistically significant at 0.016. Hence the study found that majority of the aspects of security controls influenced secure wireless network. The regression model obtained above is the enhanced framework developed that help in achieving the objective of the study. The enhanced security framework shown below:

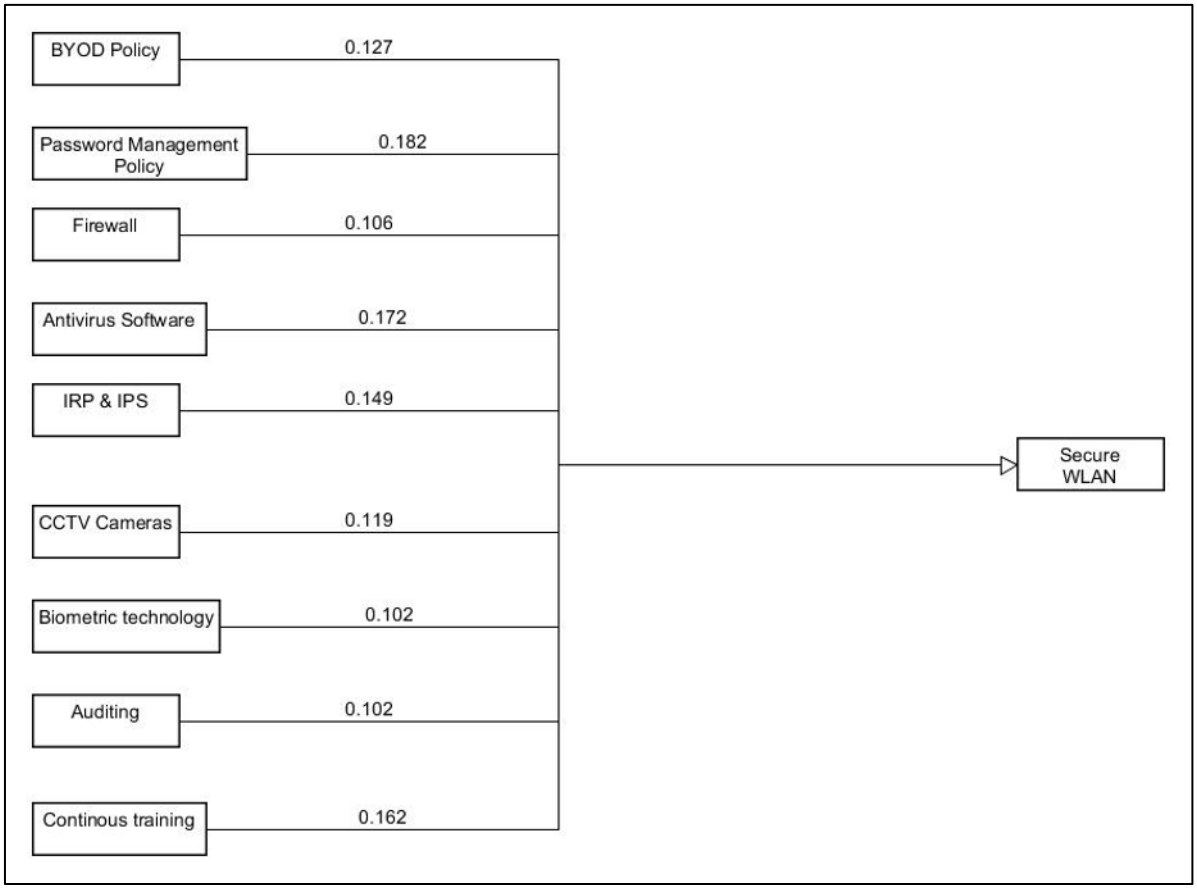

Figure 1 Enhanced Security Framework

4.3. 4.3 Validation of the developed security framework

The validation of the developed enhanced security framework for wireless network was done via looking at literature from different scholars in the domain of security frameworks.

According to [83, 84, 85, 86] an increase in consumerization of smart devices such as tablets, watches, laptops and smartphone to workplaces as made a large number of institutions to embrace the practice of Bring Your Own Device (BYOD) which as positively enhance business processes.

According to [87, 88, 89] data breaches occurs frequency due to weak password policies on major websites which is costing billions of dollars annually. Password attacks are major causes of data breaches and abuse of user accounts. Implementing and enforcing password management policies should be part and parcel of the institution social responsibility. Many technology organizations are force to beyond their internal polices to harden their password management policies in order to safe guard the account for external partners or clients with an aim of minimizing data breaches or leak of sensitive data kept on the online accounts. Moreover, enforcement of password management policies can protect organization infrastructure and resources from attacks. Having password policy in place assist staff who are using office wireless network to do work related duty to be protected against attacks but only be policies are enforced.

According to [90, 91, 92] the past few years they have been rapid development of internet and its application's which has increased the number of user online and cyber security attacks. Therefore, the internet users need to be shielded from the overgrowing attacks. Firewall which first line defense in network need to be implemented in the institution's networks.

In the modern day, internet globally used with people of different walks of life for entertainment, communication and information acquisition. Hackers also have access to the internet and they can use malicious software to compromise user privacy and sensitive files. To safe guard against such attack's antivirus software come in handy in order to minimize the risk of the device being infected hence downloading files and programs from unknown sources can lead to an infection. The use of antivirus software is very important and regular updates should be done from signature database. Antivirus software developers are always on alert on developing new security tactics and update signature databases to deal with emerging threats. Despite the great effort put by antivirus developers there is rise in numbers of new viruses which requires another level of security to be put in place to work in conjunction with antivirus software's [93, 94, 95].

Incident response plan play a major role in an organization especially when security incident occurs such as data breach, malware attack, ransomed attack or unauthorized access. A good structured incident response plan is vital to reduce the impact and restore normal organization operations. Moreover, it ensures timely detection of security incident via continuous monitoring and having it boost reputation of company. Furthermore, a good incident response and management strategies allows organization to quickly respond and mitigate the potential damages. It is conspicuous that incident response plan is key in organization and should always put in place in order to minimize loss after security incident [96, 97, 98].

According to [98, 100, 101] videos produced by surveillance cameras play crucial role in crime prevention and examination in office environment or city. Over the years the use of closed-circuit television camera (CCTV) use have been on the rise as well as evidence base on its crime prevention effect in public and private space. CCTV cameras cab used to monitor server room where network devices operate from and also access point installed various places in the organization with aim prevent theft or destruction of the devices. It noticeable the CCTV cameras are essentials security controls to prevent crime or destruction of assets in the organization furthermore they video footage can be used as evidences in court of law.

According to [102, 103, 104 ,105] in dealing with security authentication plays major role in both public and private sector such as banking system, transport systems, health systems, law and security. Biometric technology has become popular very fast especially in areas of intelligence and identity. Due to increase in fraud in recent years has made many organizations embrace the biometric technology since it very difficult to forge physical traits of person such as fingerprint, facial and retina. Biometric continues to be growing way to verify identity for security systems and it offers good solution for security. It is evident that biometric technology is vital security control when used as authentication method.

In recent years the adoption of technology has been on the rise with digitalization of almost every service which has force people to be computer literate. However, the increase dependency on digital service goes hand in hand with increased exposure to digital security threats. The number of cyber-attacks is on the rise affecting organizations and individuals the same way. Human behavior is the weakest link to cyber security thus organizations have become a common prey to attackers. Thus, continuous training is critical for creating awareness and imparting knowledge to users to ensure they operate and behave securely [106,107,108,109]. Its therefore observable that continuous training is key security control in organization.

5. Conclusion and Further research

The study was carried out successfully to achieve its objectives which were to develop an enhanced security framework for implementing secure wireless network and validate it. The study finding indicated that BYOD policy, Password management policy, Firewall, Antivirus software, Intrusion detection & intrusion protection systems, CCTV cameras, Biometric technology, Auditing and continuous training are essential security controls which must put in place in order to have secure wireless network environment. From the table 4 it can conclude that the framework can be used to explain the effect of security controls on secure wireless network as P=0.000 which is significant hence is feasible and can be used to predict the effect of the independent variable on the dependent variable. Lastly the findings of the study agreed with outputs of previous works done various researchers on the same domain.

Wireless network security is not a walk in the park but requires continuous research, training and development. This study recommends that further research be carried out to refine or expand the development of security framework further by considering institutions in other sectors such healthcare, telecommunications, Hospitality and banking. Furthermore, the study identified nine variables had a statistically significant impact on secure wireless network. The model R-squared was 70.4%, which means that 29.6% was answered by other variables not captured in the study. Thus, more studies need to be conducted on which other factors impact on secure wireless network.

Compliance with ethical standards

Disclosure of conflict of interest

There is no conflict of interest in the study.

References

[1] Nazir R, Leghari AA, Kumar K, David S, Ali M. Survey on wireless network security. Archives of Computational Methods in Engineering. 2021 Jul: 1-20.

[2] Osorio DP, Ahmad I, Sánchez JD, Gurtov A, Scholliers J, Kutila M, Porambage P. Towards 6G-enabled internet of vehicles: Security and privacy. IEEE Open Journal of the Communications Society. 2022 Jan 14; 3:82-105.

[3] Salama R, Al-Turjman F, Bhatla S, Gautam D. Network security, trust & privacy in a wired wireless Environments–An Overview. In2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) 2023 Apr 20 (pp. 812-816). IEEE.

[4] Kizza JM. Security in wireless networks and devices. In Guide to Computer Network Security 2024 Jan 20 (pp. 443-473). Cham: Springer International Publishing.

[5] Zhu L, Xiang H, Zhang K. A light and anonymous three-factor authentication protocol for wireless sensor networks. Symmetry. 2021 Dec 30; 14(1):46.,

[6] Ahmad R, Wazirali R, Abu-Ain T. Machine learning for wireless sensor networks security: An overview of challenges and issues. Sensors. 2022 Jun 23; 22(13):4730.

[7] Jabeen T, Jabeen I, Ashraf H, Jhanjhi NZ, Yassine A, Hossain MS. An intelligent healthcare system using IoT in wireless sensor network. Sensors. 2023 May 25; 23(11):5055.

[8] Baraton K. Security of Wireless Campus Networks in Selected Public and Private Universities in Kenya.

[9] Alzahrani BA, Irshad A, Albeshri A, Alsubhi K. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. Wireless Personal Communications. 2021 Mar; 117(1):47-69.

[10] Maesaroh S, Kusumaningrum L, Sintawana N, Lazirkha DP, Dinda R. Wireless network security design and analysis using wireless intrusion detection system. International Journal of Cyber and IT Service Management. 2022 Feb 7; 2(1):30-39.

[11] Faris M, Mahmud MN, Salleh MF, Alnoor A. Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management. 2023 Feb 8; 15:18479790231157220.

[12] Verma R, Bharti S. A survey of network attacks in wireless sensor networks. In International Conference on Information, Communication and Computing Technology 2020 May 9 (pp. 50-63). Singapore: Springer Singapore.

[13] Ali A, Hameed MM, Asad M, Aslam U, Pasha M, Kajla NI. Risk and Security Attacks in Physical Layer of IoT Environment. STATISTICS, COMPUTING AND INTERDISCIPLINARY RESEARCH. 2024 Jun 30; 6(1):91-112.

[14] Ee SJ, Ming JW, Yap JS, Lee SC, tuz Zahra F. Active and passive security attacks in wireless networks and prevention techniques. Authorea Preprints. 2023 Sep 11.

[15] Silva-Trujillo AG, González González MJ, Rocha Pérez LP, García Villalba LJ. Cybersecurity analysis of wearable devices: smartwatches passive attack. Sensors. 2023 Jun 8; 23(12):5438.

[16] Rani V. Review Paper On Security issues in Wireless LAN. International.

[17] Al-Shareeda MA, Anbar M, Manickam S, Hasbullah IH. Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. International Journal of Engineering and Management Research. 2020 Jul 29; 10.

[18] Nemec Zlatolas L, Welzer T, Lhotska L. Data breaches in healthcare: security mechanisms for attack mitigation. Cluster Computing. 2024 Apr 13:1-6.

[19] Shi L, Liu Q, Shao J, Cheng Y. Distributed localization in wireless sensor networks under denial-of-service attacks. IEEE Control Systems Letters. 2020 Jun 19; 5(2):493-8.

[20] Bhardwaj A, Mangat V, Vig R, Halder S, Conti M. Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review. 2021 Feb 1; 39:100332.

[21] Uddin R, Kumar SA, Chamola V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks. 2024 Jan 1; 152:103322.

[22] Yousef D, Maala B, Skvortsova M, Pokamestov P. Detection of non-periodic low-rate denial of service attacks in software defined networks using machine learning. International Journal of Information Technology. 2024 Apr; 16(4):2161-75.

[23] Raoof A, Matrawy A, Lung CH. Routing attacks and mitigation methods for RPL-based Internet of Things. IEEE Communications Surveys & Tutorials. 2018 Dec 9; 21(2):1582-606.

[24] Gowda S, Dayananda RB. Detection and Prevention of ARP Attack in Software Defined Networks. In2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) 2023 Jul 6 (pp. 1-5). IEEE.

[25] Raoof A, Matrawy A, Lung CH. Routing attacks and mitigation methods for RPL-based Internet of Things. IEEE Communications Surveys & Tutorials. 2018 Dec 9; 21(2):1582-606.

[26] Owolafe O, Adediran GM, Ayeni OA. Rogue Access Detection Using Multi-Parameter Dynamic Features on WLAN. In Privacy Preservation and Secured Data Storage in Cloud Computing 2023 (pp. 458-474). IGI Global.

[27] Yang Z, Lu Q, Zhang H, Chen F, Xian H. Eliminating Rogue Access Point Attacks in IoT: A Deep Learning Approach With Physical-Layer Feature Purification and Device Identification. IEEE Internet of Things Journal. 2023 Dec 21.

[28] Zulkipli NH, Khusairi MI. An Experimental Analysis for Public Wi-Fi Attacks. In2024 IEEE 6th Symposium on Computers & Informatics (ISCI) 2024 Aug 10 (pp. 247-252). IEEE.

[29] Butun I, Österberg P, Song H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials. 2019 Nov 13; 22(1):616-44.

[30] Chen Y, Li W, Cheng X, Hu P. A survey of acoustic eavesdropping attacks: Principle, methods, and progress. High-Confidence Computing. 2024 May 18:100241.

[31] Fu X, Wen G, Niu M, Zheng WX. Distributed secure filtering against eavesdropping attacks in SINR-based sensor networks. IEEE Transactions on Information Forensics and Security. 2024 Feb 1.

[32] Lu L, Chen M, Yu J, Ba Z, Lin F, Han J, Zhu Y, Ren K. An Imperceptible Eavesdropping Attack on WiFi Sensing Systems. IEEE/ACM Transactions on Networking. 2024 May 28.

[33] Kausar F, Aljumah S, Alzaydi S, Alroba R. Traffic analysis attack for identifying users' online activities. IT Professional. 2019 Mar 28; 21(2):50-7.

[34] Wu Y, Xiang Y, Baker T, Tong E, Zhu Y, Cui X, Zhang Z, Han Z, Liu J, Niu W. Collaborative Attack Sequence Generation Model Based on Multiagent Reinforcement Learning for Intelligent Traffic Signal System. International Journal of Intelligent Systems. 2024; 2024(1):4734030.

[35] Hussain K, Rahmatyar AR, Riskhan B, Sheikh MA, Sindiramutty SR. Threats and Vulnerabilities of Wireless Networks in the Internet of Things (IoT). In2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) 2024 Jan 8 (pp. 1-8). IEEE.

[36] Caballero-Gil C, Alvarez R, Hernández-Goya C, Molina-Gil J. Research on smart-locks cybersecurity and vulnerabilities. Wireless Networks. 2024 Aug; 30(6):5905-17.

[37] Zahra FT, Bostanci YS, Soyturk M. Security of Wireless IoT in Smart Manufacturing: Vulnerabilities and Countermeasures. InIntelligent Secure Trustable Things 2024 Jun 20 (pp. 419-441). Cham: Springer Nature Switzerland.

[38] Narwal B, Mohapatra AK. A survey on security and authentication in wireless body area networks. Journal of Systems Architecture. 2021 Feb 1; 113:101883.

[39] Moissinac K, Ramos D, Rendon G, Elleithy A. Wireless encryption and WPA2 weaknesses. In2021 IEEE 11th Annual computing and communication workshop and conference (CCWC) 2021 Jan 27 (pp. 1007-1015). IEEE.

[40] Easttom C. Virtual private networks, authentication, and wireless security. In Modern Cryptography: Applied Mathematics for Encryption and Information Security 2022 Oct 30 (pp. 309-327). Cham: Springer International Publishing.

[41] Phalaagae P, Zungeru AM, Sigweni B, Rajalakshmi S. Authentication schemes in wireless internet of things sensor networks: a survey and comparison. Indonesian Journal of Electrical Engineering and Computer Science. 2024 Mar; 33(3):1876-88.

[42] Alexandrou A, Chen LC. Perceived security of BYOD devices in medical institutions. International Journal of Medical Informatics. 2022 Dec 1; 168:104882.

[43] Ratchford M, El-Gayar O, Noteboom C, Wang Y. BYOD security issues: A systematic literature review. Information Security Journal: A Global Perspective. 2022 May 4; 31(3):253-73.

[44] Datta AN, Abhi S, Kumar N. Enhancing BYOD Security: A Risk Assessment Framework for Corporate Resources. InInternational Conference on Computing and Machine Learning 2024 Mar 29 (pp. 483-496). Singapore: Springer Nature Singapore.

[45] Halim II, Buja AG, Zain JM, Ngah AH, Bansal R. BYOD Security Policy Model: A Systematic Literature Review. Journal of Advanced Research in Applied Sciences and Engineering Technology. 2024 Oct 14:170-86.

[46] Azam H, Tan M, Pin LT, Syahmi MA, Qian AL, Jingyan H, Uddin MF, Sindiramutty SR. Wireless Technology Security and Privacy: A Comprehensive Study.

[47] Zhang X, Klevering G, Lei X, Hu Y, Xiao L, Tu GH. The security in optical wireless communication: A survey. ACM Computing Surveys. 2023 Jul 17; 55(14s):1-36.

[48] Kutay E, Yener A. Classification-oriented semantic wireless communications. InICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2024 Apr 14 (pp. 9096-9100). IEEE.

[49] Nazir R, Laghari AA, Kumar K, David S, Ali M. Survey on wireless network security. Archives of Computational Methods in Engineering. 2021 Jul: 1-20.

[50] Liu YA, Zhang L. Enhancing secondary recovery in microgrid: Event-driven robust security control with semi-Markov switched dynamics. Applied Mathematics and Computation. 2024 Oct 1; 478:128838.

[51] Taherdoost H. Privacy and security of blockchain in healthcare: applications, challenges, and future perspectives. Sci. 2023 Oct 30; 5(4):41.

[52] Elkourdi F, Wei C, Xiao L, Yu Z, Asan O. Exploring Current Practices and Challenges of HIPAA Compliance in Software Engineering: Scoping Review. IEEE Open Journal of Systems Engineering. 2024 Apr 23.

[53] Ansari MF, Dash B, Swayamsiddha S, Panda G. Use of blockchain technology to protect privacy in electronic health records-a review. In2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) 2023 Jan 5 (pp. 144-149). IEEE.

[54] Akter MS, Barek MA, Rahman MM, Riad AK, Rahman MA, Mia MR, Shahriar H, Chu W, Ahamed SI. HIPAA Technical Compliance Evaluation of Laravel-based mHealth Apps. In2024 IEEE International Conference on Digital Health (ICDH) 2024 Jul 7 (pp. 58-67). IEEE.

[55] Nurdin A, Lubis M. The IT Governance Measurement using Cobit 5 Framework in Quality Assurance Department. Jurnal Informatika dan Rekayasa Perangkat Lunak. 2023 Mar 31; 5(1):80-8.

[56] Adhari MF, Setiawan J. IT Governance Assessment at City Revenue Agency Using COBIT 5 Framework. Journal of Information Systems and Informatics. 2024 Sep 30; 6(3):2159-72.

[57] Sang K. Cybersecurity Assessment Model for Small and Medium Enterprises (Smes) E-commerce in Kenya (Doctoral dissertation, Kca University).

[58] Ilori O, Nwosu NT, Naiho HN. A comprehensive review of it governance: effective implementation of COBIT and ITIL frameworks in financial institutions. Computer Science & IT Research Journal. 2024 Jun 14; 5(6):1391-407.

[59] Venkatachary SK, Prasad J, Alagappan A, Andrews LJ, Raj RA, Duraisamy S. Cybersecurity and Cyber-terrorism Challenges to Energy-Related Infrastructures-Cybersecurity Frameworks and Economics–Comprehensive review. International Journal of Critical Infrastructure Protection. 2024 Apr 21:100677.

[60] Chen H, Yang D, Zhang JH, Zhou H. Internal controls, risk management, and cash holdings. Journal of Corporate Finance. 2020 Oct 1; 64:101695.

[61] Liu X, Wang J, Guo S, Wang H. A Survey on Cross-Layer Authentication in Wireless Communication Networks. Journal of Networking and Network Applications. 2024 Apr 22; 4(1):21-30.

[62] Gudala L, Shaik M, Venkataramanan S. Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies. Journal of Artificial Intelligence Research. 2021 Nov 26; 1(2):19-45.

[63] Ojha NK, Baray E. An Overview of Protocols-Based Security Threats and Countermeasures in WLAN. In2023 4th International Conference for Emerging Technology (INCET) 2023 May 26 (pp. 1-6). IEEE.

[64] Zhang, J., Zhang, Q., Li, Z., Lu, X., & Gan, Y. (2021). A Lightweight and Secure Anonymous User Authentication Protocol for Wireless Body Area Networks. Security and Communication Networks, 2021, 1-11.

[65] Zhu, L., Xiang, H., & Zhang, K. (2021). A Light and Anonymous Three-Factor Authentication Protocol for Wireless Sensor Networks. Symmetry, 14(1), 46

[66] Syed, F. M., & ES, F. K. (2023). Leveraging AI for HIPAA-Compliant Cloud Security in Healthcare. Revista de Inteligencia Artificial en Medicina, 14(1), 461-484.

[67] Lee TF, Chang IP, Su GJ. Compliance with hipaa and gdpr in certificateless-based authenticated key agreement using extended chaotic maps. Electronics. 2023 Feb 23; 12(5):1108.

[68] Salunkhe V, Thakur D, Krishna K, Goel O, Jain P. Optimizing Cloud-Based Clinical Platforms Best Practices for HIPAA and HITRUST Compliance. Arpit, Optimizing Cloud-Based Clinical Platforms Best Practices for HIPAA and HITRUST Compliance (December 30, 2023). 2023 Dec 30.

[69] Oakley A. HIPAA, HIPPA, or HIPPO: What Really Is the Heath Insurance Portability and Accountability Act?. Biotechnology Law Report. 2023 Dec 1; 42(6):306-18.

[70] Lincke S. Complying with the PCI DSS Standard. In Information Security Planning: A Practical Approach 2024 Jan 17 (pp. 45-63). Cham: Springer International Publishing.

[71] Nurdin A, Lubis M. The IT Governance Measurement using Cobit 5 Framework in Quality Assurance Department. Jurnal Informatika dan Rekayasa Perangkat Lunak. 2023 Mar 31; 5(1):80-8.

[72] Amali LN, Katili MR, Suhada S, Hadjaratie L. The measurement of maturity level of information technology service based on COBIT 5 framework. Telkomnika (Telecommunication Computing Electronics and Control). 2020 Feb 1; 18(1):133-9.

[73] Tangka GM, Liem AT, Mambu JY. Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University. In2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS) 2020 Oct 27 (pp. 1-5). IEEE.

[74] Monev V. Organisational information security maturity assessment based on ISO 27001 and ISO 27002. In2020 International Conference on Information Technologies (InfoTech) 2020 Sep 17 (pp. 1-5). IEEE.

[75] Alexei A. Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. Journal of Social Sciences. 2021; 4(1):84-94.

[76] Ryanto K, Tundjungsari V. Standardization of Information Security Management in the Banking Sector using the ISO 27001: 2022 Framework. Journal La Multiapp. 2024 Aug 6; 5(4):361-79.

[77] Kitsios F, Chatzidimitriou E, Kamariotou M. The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. Sustainability. 2023 Mar 27; 15(7):5828.

[78] Hasibovic AC, Tanovic A. Review of ISO 9001: 2015 and ISO 27001: 2013 Implementation in Financial Institution–Case Study. In2024 47th MIPRO ICT and Electronics Convention (MIPRO) 2024 May 20 (pp. 1520-1525). IEEE.

[79] Wijaya AI, Lestiani DI, Damayanti YR, Sugiono AA, Huanggino SC. Maturity Level Risk Assessment in Media Companies Using the ISO 27001 Framework. Journal of Digital Business and Innovation Management. 2024 Jun 30; 3(1):1-20.

[80] Moller DP. NIST cybersecurity framework and MITRE cybersecurity criteria. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices 2023 Apr 19 (pp. 231-271). Cham: Springer Nature Switzerland.

[81] Alshar'e M. Cyber security framework selection: Comparison of NIST and ISO27001. Applied computing Journal. 2023 Feb 9:245-55.

[82] Mugenda OM, Mugenda AG. Research methods: Quantitative & qualitative approaches. Nairobi: Acts press; 2003.

[83] Mbithi M, Kihara P, Omanwa CN. Operational Processes and Performance of private chartered Universities in Kenya. Reviewed Journal International of Business Management [ISSN 2663-127X]. 2024 Jul 5; 5(1):344-51.

[84] Downer K, Bhattacharya M. BYOD security: A study of human dimensions. In Informatics 2022 Feb 23 (Vol. 9, No. 1, p. 16). MDPI.

[85] Njuguna D, Kanyi W. An evaluation of BYOD integration cybersecurity concerns: A case study. Int. J. Recent Res. Math. Comput. Sci. Inf. Technol. 2023; 9:80-91.

[86] Halim II, Buja AG, Zain JM, Ngah AH, Bansal R. BYOD Security Policy Model: A Systematic Literature Review. Journal of Advanced Research in Applied Sciences and Engineering Technology. 2024 Oct 14:170-86.

[87] Wani TA, Mendoza A, Gray K. BYOD Security Practices in Australian Hospitals–A Qualitative Study. InInternational Conference on Human-Computer Interaction 2024 Jun 1 (pp. 138-158). Cham: Springer Nature Switzerland.

[88] West T. Weak Password Policies: A Lack of Corporate Social Responsibility. In Journal of the Colloquium for Information Systems Security Education 2020 Dec 1 (Vol. 8, No. 1, pp. 8-8).

[89] Lee K, Sjöberg S, Narayanan A. Password policies of most top websites fail to follow best practices. In Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022) 2022 (pp. 561-580).

[90] Fernando WP, Dissanayake DA, Dushmantha SG, Liyanage DL, Karunatilake C. Challenges and Opportunities in Password Management: A Review of Current Solutions. Research Gate. 2023 Aug 21.

[91] Anwar RW, Abdullah T, Pastore F. Firewall best practices for securing smart healthcare environment: A review. Applied Sciences. 2021 Oct 2; 11(19):9183.

[92] Rajkumar B, Arunakranthi G. Evolution for a secured path using NexGen firewalls. In2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON) 2023 Feb 8 (pp. 1-6). IEEE.

[93] Bringhenti D, Valenza F. Greenshield: Optimizing firewall configuration for sustainable networks. IEEE Transactions on Network and Service Management. 2024 Aug 30.

[94] Drakulic U, Mujcic E. A Comparative Performance Analysis of Various Antivirus Software. InInternational Symposium on Innovative and Interdisciplinary Applications of Advanced Technologies 2023 Jun 1 (pp. 423-430). Cham: Springer Nature Switzerland.

[95] Samociuk D. Antivirus evasion methods in modern operating systems. Applied Sciences. 2023 Apr 19; 13(8):5083.

[96] Ryu Y, Shin K, Lee J, Jung DJ, Cho HM. Real-World Antivirus Evaluation Methodology: Applying Modern Criteria for Assessing Antivirus Functionality. In2024 International Conference on Information Networking (ICOIN) 2024 Jan 17 (pp. 783-788). IEEE.

[97] Shinde N, Kulkarni P. Cyber incident response and planning: a flexible approach. Computer Fraud & Security. 2021 Jan; 2021(1):14-9.

[98] Ahmad A, Maynard SB, Desouza KC, Kotsias J, Whitty MT, Baskerville RL. How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security. 2021 Feb 1; 101:102122.

[99] Farok NA, Zolkipli MF. Incident Response Planning and Procedures. Borneo International Journal eISSN 2636-9826. 2024 Jun 25; 7(2):69-76.

[100] Matczak P, Wójtowicz A, Dąbrowski A, Mączka K. Cost-effectiveness of CCTV surveillance systems: Evidence from a Polish city. European Journal on Criminal Policy and Research. 2023 Dec; 29(4):555-77.

[101] Ahmad AY. Fraud Prevention in Insurance: Biometric Identity Verification and AI-Based Risk Assessment. In2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS) 2024 Apr 18 (Vol. 1, pp. 1-6). IEEE.

[102] Eliazer M, Mudgil Y, Bachu DG. Smart CCTV camera surveillance system. InAIP Conference Proceedings 2024 Jul 29 (Vol. 3075, No. 1). AIP Publishing.

[103] Bai L, Zhu L, Liu J, Choi J, Zhang W. Physical layer authentication in wireless communication networks: A survey. Journal of Communications and Information Networks. 2020 Sep 21; 5(3):237-64.

[104] Narwal B, Mohapatra AK. A survey on security and authentication in wireless body area networks. Journal of Systems Architecture. 2021 Feb 1; 113:101883.

[105] Modi K, Devaraj L. Advancements in biometric technology with artificial intelligence. arXiv preprint arXiv:2212.13187. 2022 Dec 16.

[106] Wang D, Zhou J, Masdari M, Qasem SN, Sayed BT. Security in wireless body area networks via anonymous authentication: Comprehensive literature review, scheme classification, and future challenges. Ad Hoc Networks. 2024 Feb 1; 153:103332.

[107] Alsharida RA, Al-rimy BA, Al-Emran M, Zainal A. A systematic review of multi perspectives on human cybersecurity behavior. Technology in society. 2023 May 1; 73:102258.

[108] Kannelonning K, Katsikas SK. A systematic literature review of how cybersecurity-related behavior has been assessed. Information & Computer Security. 2023 Oct 30; 31(4):463-77.

[109] Kavrestad J, Furnell S, Nohlberg M. User perception of Context-Based Micro-Training–a method for cybersecurity training. Information Security Journal: A Global Perspective. 2024 Mar 3; 33(2):121-37.