Journal of Information Systems and Informatics
Vol. 7, No. 3, September 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i3.1155 Published By DRPM-UBD

Enhancing the Security of Internet of Things Devices through Cybersecurity Framework

Godfrey M. Macharia[1], Bonny Mgawe[2], Jaha Mvula[3], Anael E. Sam[4]

[1,2,4]The Nelson Mandela African Institution of Science and Technology, Tanzania
[3]Electronic Government Authority, Tanzania
Email: [1]machariag@nm-aist.ac.tz, [2]anael.sam@nm-aist.ac.tz,
[3]bonny.mgawe@nm-aist.ac.tz, [4]jaha.mvula@ega.go.tz

Abstract

This study focused on enhancing the protection of IoT devices by assessing the effectiveness of existing cybersecurity frameworks (CSFs), identifying gaps in advanced technology cyber-attack tactics, and developing a comprehensive cybersecurity framework for IoT ecosystems. Technological Acceptance and Zero Trust Security Theories guided the study. A cross-sectional research design and mixed-methods approach was adopted, while semi-structured interviews and Focus Group Discussions provided in-depth qualitative insights. For quantitative data, a questionnaire was used. A total of 93 respondents from HLIs, hospitals, and broadcasting media were selected using purposive and random sampling techniques. Descriptive and inferential statistics were employed to analyze quantitative data. For qualitative data, Atlas.ti 9.0 Desktop was used. The findings revealed cyber vulnerabilities are associated with the spread of imported unsecured IoT devices, user unawareness, and lack of effective cybersecurity frameworks tailored to emerging cyber threats from advanced technologies such as AI, 5G, Edge computing, and Autonomous Systems. In conclusion, a framework was designed to strengthen IoT device security by integrating best practices, policy implementation, and technological safeguards. The study recommends that imported IoT devices should be digitally coded to detect cyber risks and adopt multi-layered ECSF-IoT framework and strengthen end-user cybersecurity education in developing countries such as Tanzania.

Keywords: Cybersecurity Framework, Internet of Things, Technological Acceptance Theory, Zero Trust Theory

1. INTRODUCTION

The Internet of Things (IoT) is among the most advanced and the fastest-growing technologies worldwide, offering improved efficiency, automation, and increased ease of operations across various sectors such as education,

healthcare, smart agriculture, and smart cities [1]. Kevin Ashton introduced IoT in 1999 as a remarkable phenomenon from the previous decades. IoT involves a network of connected devices that communicate with each other and with people to perform intelligent tasks [2] [3]. Nowadays, major companies like Apple and Samsung depend greatly on IoT, with global projections estimating 50 billion devices in use by the end of 2023 [4].

However, rapid expansion of IoT also introduces significant security risks especially on data, both in transit and at rest. The growing number of devices connected to the internet increases vulnerability to cyber threats, such as Distributed Denial of Service (DDoS) attacks and malware[4] [5]. According to a study by [6] modern information and communication technology (ICT) systems are more advanced and complicated but also vulnerable, which invites cyber criminals to develop new attack techniques DDoS and DoS represent the most common and critical attack against and from the IoT networks whereby methods rose by 31% in 2021 compared to the previous year [7].

Additionally, Kariakoo market in Tanzania as the leading business center in East Africa, demonstrated phishing attacks targeting mobile phone users many of whom access IoT enabled services causing substantial financial losses, reduced trust in digital communications and heightened psychological distress among victims [8]. In Arusha region, it was established that reasons of cyber-attacks are due to low level of security awareness among digital users, exposure to data breaches of confidentiality and unauthorized access [9]. Furthermore, the 2023 Bank of Tanzania (BoT) report on the National Payment Systems highlights emerging technologies like cryptocurrencies, 5G Internet services and Distributed Ledgers Technologies as among used yet posing significant cyber risks to unprepared mobile banking customers and thus requires new approaches to address cyberattack challenges due to phishing and malware threats [10].

In reducing cyber risks several frameworks have been proposed to address these challenges. One of the most recognized Cybersecurity Framework (CSF) developed by the United States of America is the National Institute of Standards and Technology (NIST) Cybersecurity framework, which provides guidelines to help organizations manage and reduce cybersecurity risks [11]. Existence of cyber security frameworks is to ensure confidentiality, integrity, and availability of systems [12], emphasizing the need for secure hardware, software, and layered security protocols [13].

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Even though efforts have been implemented, there are still notable unresolved cyber issues that need further and different approaches to solve them. Earlier scholarly work and existing frameworks do not fully address the fast-changing nature of cyberattacks, especially for the case of African IoT users, whereby awareness, infrastructure, and resources are limited [14] [15]. In Tanzania, cyber-attacks have significantly increased in recent years, attacks in private and government institutions, Industries, Websites and sensitive institutions of education such as the Tanzania Commission for Universities (TCU). More than 900,000 network attacks were reported by the Tanzania Computer Emergency Response Team (TZ-CERT) in 2024 alone [16]. Even though national strategies such as the Cyber Security Strategy (2022–2027) have been launched, sectors like health, banking, and education continue to face cyber threats due to lack of technical know-how from IoT devices users, use of imported unsecured devices, and weak technical safeguards [17] [18].

Most of the existing studies focus on individual component vulnerability in IoT systems but lack comprehensive framework that take into account for the recent technological advancements associated from emerging technological cyber threats such as Artificial Intelligence (AI), 5G Technology, Cloud computing and Autonomous systems. For instance, [19] and [20] highlighted the layered structure of IoT and its security concern, there is limited observation on how IoT users in developing countries such as Tanzania, manage these threats in real-life environments. Limited computational resources and lack of protocol standardization as IoT devices integrates with many other systems make a clear view of security challenges in the making of one structured cybersecurity framework [21]. A study by [22] shows that 40% of East African banks were inadequately prepared to counter cyber threats as these institutions integrated into computerized operations, as well as using advanced digital systems and tools.

This study identifies an important gap by focusing on the urgent need for a cybersecurity framework that is specifically designed for the realities of developing countries like Tanzania. While many existing studies and frameworks, such as NIST, provide general guidelines for securing IoT systems, they often overlook key background factors such as limited infrastructure and computational resources, low cyber security awareness among users, and emerging cyber threats due to advancement technology [21]. Existing literatures show inadequately technical aspects with little consideration on how human behavior and the widespread use of imported, low-security IoT devices increase vulnerability [15] [23]. Therefore, this study provides an approach not only in evaluating the effectiveness of existing

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

frameworks available in Tanzania but also by proposing an Enhanced Cybersecurity Framework for IoT devices (ECSF-IoT) for enabling security of IoT ecosystem. The framework aims to integrate technological features of IoT devices with practical concerns, including user behavior, policy enforcement and implementation, and security recommendation, hence offering a more comprehensive and realistic solution to improving IoT cyber security in Tanzania.

2. METHODS

This study employed a mixed-methods approach, combining qualitative and quantitative techniques to understand human experience and statistically test hypotheses [24]. A cross-sectional design integrated literature review, field surveys, semi-structured interviews, focus groups, documentary reviews, and cyber-crime statistical analysis [25]. This integration strengthened findings by providing measurable evidence and contextual insights into IoT device security challenges. Quantitative analysis validated vulnerabilities and attack patterns, while qualitative data revealed user behaviors and perceptions affecting security practices. These methods enhanced the reliability and applicability of the proposed IoT cybersecurity framework for Tanzania through comprehensive exploration and data cross-validation.

2.1. Literature Review

Relevant literature was reviewed to explore procedural and technical aspects of cybersecurity frameworks in the context of IoT. Technological Acceptance Theory, proposed by Fred Davis in 1989, guided the study. The theory suggests that the intention of people to accept and use technology is determined by two factors: perceived ease of use and perceived usefulness [26].The theory suggests that the use of information technology depends on behaviour intention, and behaviour intention depends on personal attitude towards the use of the system and their perception of its usefulness or utility [27]. User attitudes and beliefs are important features that influence the new technology's use. Therefore, perceived ease of use by IoT users in HLIs, hospitals and broadcasting media greatly affect the adoption and implementation of cyber security framework designed guidelines.

2.2. Survey and Field Data Collection

A structured questionnaire was used to gather quantitative data from ICT and Cyber experts across three major urban regions, Dar es Salaam, Dodoma, and Arusha. These regions were purposively selected for their

technological infrastructure and IoT device penetration. According to Tanzania Investment and Consultant Group Ltd (TICGL) these regions are among the leading five regions in Tanzania expanding mobile subscriptions, infrastructure and digital connectivity in machine-to-machine, IoTs, the number of telecommunication towers and availability of communication masts up to 5G.

2.3. Interviews and Focus Group Discussions

Semi-structured interviews and Focus Group Discussions provided meaningful, in-depth qualitative insights into participants' experiences perspectives, beliefs and behaviours for the existing cyber security challenges [28]. Most common methods of data collection used in qualitative research are interviews and focus groups which were previously conducted face to face but evolution of technologies has further helped through video chat and online forums.

2.4. Data Analysis

Through structured questionnaires quantitative data were analyzed using SPSS for descriptive and inferential statistics, identifying patterns, frequencies, relationships and data visualization [29] (Jalolov, 2024). From discussion, interviews, documentaries and documents, thematic analysis was used to interpret qualitative data using Atlas.ti 9.0 Desktop for unstructured, non-numerical textual documents producing code-based content which involve three stages of thematic content analysis: pre-analysis, material exploration and interpretation within the software's intuitive interface [30].

2.5. Sample Size

Sample size refers to the number of data points selected from the entire target individuals that are considered representative of the real population for that specific study [31]. This study used Yamane formula to draw its sample size from the target population. Yamane Formula which states: $n=\frac{N}{1+N(e)^2}$ [32].

Whereby
n= required sample size, therefore:
N= target population and
e= margin error (0.1 or 10%)

$$n=\frac{1328}{1+1328(0.1)^2}$$

$$n=92.735\approx 93$$

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Hence, a total of 93 participants were selected using a combination of purposive and random sampling techniques: 15 ICT officers from higher education institutions, 12 from hospitals, and 4 from broadcasting media per region. The healthcare, broadcasting media and higher learning sectors are critical to national infrastructure and increasingly adopt IoT devices, each facing unique cybersecurity challenges. Healthcare deals with sensitive patient data and life critical equipment that requires more reliable cybersecurity. Moreover, broadcasting media relies on IoT for content delivery and communications nonetheless they are vulnerable to disruptions and misinformation. In addition, HLIs use IoT across research and administration that requires safety measures against cyberattacks. Consequently, these sectors in Tanzania should comprehensively address IoT cybersecurity challenges by using new approach against cyberattacks.

2.6. Research Steps

Based on Figure 1, the researcher employed a mixed methods approach, combining quantitative and qualitative techniques to study security challenges for IoT devices. Simple random and purposive sampling techniques were employed to select respondents. Data were gathered through questionnaires, interviews, focus groups, and document reviews to ensure data triangulation. Qualitative data were analyzed thematically using ATLAS.ti 9.0 desktop, while quantitative survey data were processed with SPSS 27. The findings identified key IoT vulnerabilities and controls, informing the developed framework design, which was then validated by cybersecurity experts to ensure its practical relevance and theoretical robustness.

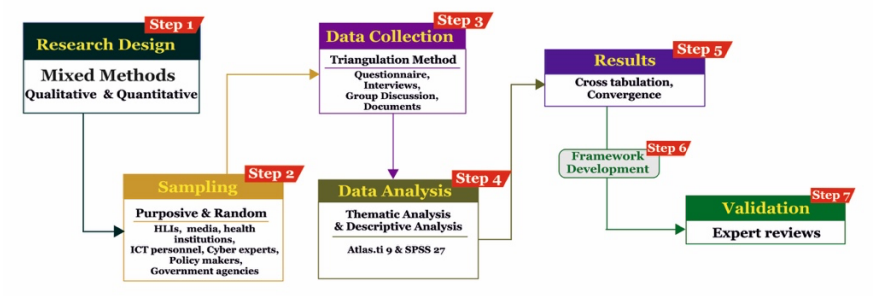

Figure 1. Research Stages: Adopted and Modified [33]

Based on Figure 1, the explanation as follow.

1) Step 1: Research Design - by integrating numerical data analysis with in-depth contextual understanding, researcher used a mixed methods

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

research design combining both quantitative and qualitative methodologies within a single study to comprehensively answer research questions.

2) Step 2: Sampling – participants were chosen at random from sectors identified to guarantee every respondent of the population equal chance to be selected. For purposeful sampling which is a non-probability technique, participants were specifically chosen based on individual characteristics in relation to the study objectives whereby ICT personnel and cyber security experts were involved.
3) Step 3: Data Collection – researcher used multiple methods such as interviews, questionnaires, documents reviews and group discussions to access diverse data sources, enhancing in-depth, validity, and reliability of the research findings.
4) Step 4: Data Analysis - researcher analyzed qualitative data thematically using ATLAS.ti 9 desktop and processed quantitative survey data statistically with SPSS 27, combining detailed textual insights with strong numerical analysis.
5) Step 5: Results – in addition, the researcher identified key IoT vulnerabilities and effective controls through the developed framework, which guided the creation of a comprehensive cybersecurity framework subsequently validated by experts for its practical relevance and theoretical reliability.
6) Step 6: Framework development - the researcher developed the ECSF-IoT framework using a mixed-methods approach with thematic analysis in ATLAS.ti and statistical analysis in SPSS to identify IoT vulnerabilities and controls, resulting in an expert-validated, comprehensive cybersecurity framework.
7) Step 7: Validation – Finally, researcher validated the ECSF-IoT framework through structured expert reviews by cybersecurity professionals, ensuring its practical relevance and theoretical reliability in line with established best practices of framework validation in IoT security research.

3. RESULTS AND DISCUSSION

3.1. Socio Demographic Information of the Participants

Participants were drawn from sectors of security companies, health institutions, broadcasting media, and regulatory bodies across Tanzania, providing a broad perspective on IoT security practices and challenges. Specifically, 2 cyber experts were selected from security companies, 2 cyber experts from broadcasting media, 3 cyber experts from health institutions,

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

and 1 IoT cybersecurity specialist, all purposively selected for their subject matter of expertise. The remaining 43 professionals were randomly chosen from key regions of Dar es Salaam, Arusha, and Dodoma, which are the center to country's digital and technological development.

Most of participants had more than three years of professional experience in ICT and cybersecurity related roles which reflect both theoretical and practical proficiency in the field. This combination of technical qualifications and sectoral diversity ensured that the data collected was grounded in real world experience. The participants varied backgrounds provide valuable insights from the existing cybersecurity frameworks and highlighted the necessary achieving framework to address the security needs of IoT devices.

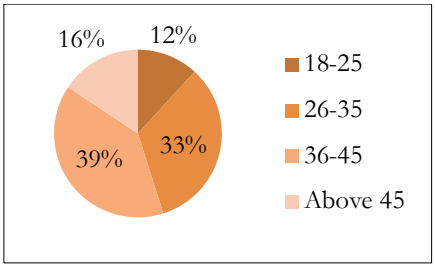

Figure 2. Age Distribution

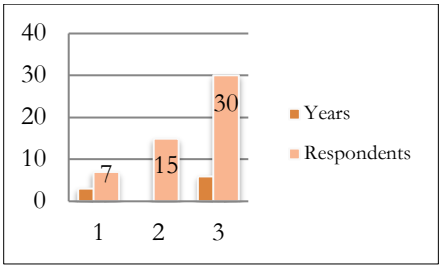

Figure 3. IoT Working Experience

On the age distribution respondents, illustration of Figure 2, observed that majority of respondents fall within the 36–45 age group (39%), which corresponds to 58.8% (30) of respondents who had over 6 years of ICT working experience, enhancing the credibility of their input in the study. Experience of respondents provided a valid observation for the existence of cybersecurity frameworks within institutions which recorded that 41.5% existence of CSF and 59.5% does not exist as illustrated in Figure 4. shows that majority of institutions are lacking formal CSFs, exposing them to significant cyber threats risks.

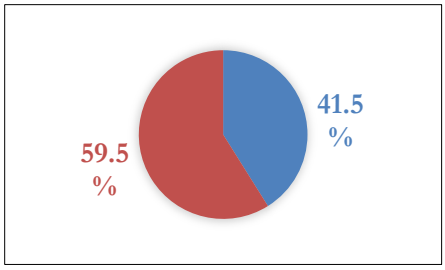

Figure 4. Existence of Cyber security Framework

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

The study involved data collection through questionnaires, interviews, and focus group discussions from ICT stakeholders, including cybersecurity experts, ICT officers, and administrators. A total of 75 instruments were distributed, and 68 were successfully collected, producing an overall response rate of 92%**.** A 92% return rate suggests effective follow up strategies and well understood instruments, supporting [34] emphasized researcher and research participants engagement as key to higher response rates

3.2. Quantitative Analysis on the Effectiveness for Existing Cyber-Security Frameworks

Quantitative analysis provided better analysis of assessing the strengths and limitations of cybersecurity framework on performance metrics such as threat identification, detection, response, accuracy and recovery.

Cybersecurity framework's effectiveness rate on the Internet of Things recognizing that the mere existence of a cybersecurity framework is insufficient without its effective execution, the study sought to evaluate the actual effectiveness of current cybersecurity frameworks (CSFs) in preventing cyberattacks. Respondents were asked to score how well their current CSFs addressed the security of their systems. According to the findings, only 13.2% of respondents thought their systems were very well covered, while 26.4% said they were fairly covered. On the other hand, 11.3% stated their systems were completely uncovered, 15.1% said they were just partially covered, and 34.0% said their systems were only partially covered. With most replies falling below the "well covered" threshold, these findings show a notable disparity in the perceived efficacy of contemporary CSFs. The majority of replies fell below the "well covered" criteria, highlighting a considerable gap in the perceived effectiveness of present CSFs and suggesting that information systems are not fully protected by the frameworks in place.

This poor performance raises the possibility that many organizations are using frameworks that are incompatible with their operational structures or that they lack the technical know-how to make effective use of them. Full adoption and optimization of these frameworks are severely hampered by their complexity, expense, and need for qualified personnel. Therefore, even while CSFs are crucial instruments for improving cybersecurity, how well they are applied, integrated, and managed within the organization will determine how much of an impact they actually have.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

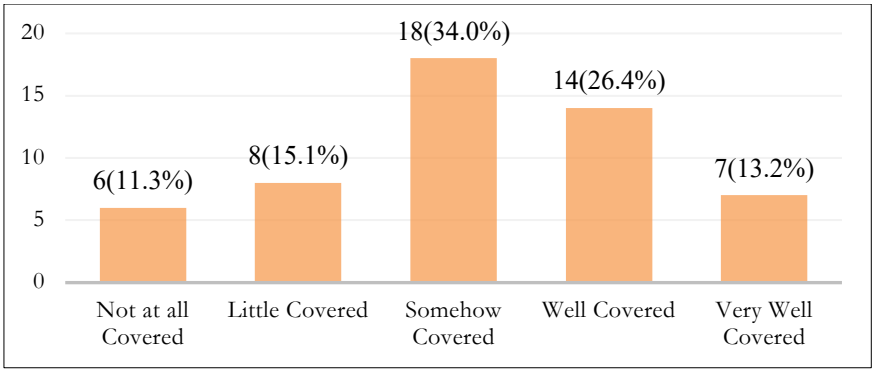

Figure 5. Security Coverage for Existing Cyber-security Framework

In order to determine the necessity of an efficient cybersecurity framework (CSF), the study also evaluated the frequency and kind of cyberattack incidents that target IoT devices. The most frequent risks were found to be social engineering (43.4%) and botnet attacks (24.5%), with physical tempering (11.3%) and a tiny fraction of combined attacks coming in second and third, respectively. These results show that human mistake, antiquated systems, complicated network endpoints, and a lack of cybersecurity measures continue to make IoT devices susceptible, especially in delicate settings like healthcare. The variety and frequency of these assaults highlight the need for more robust and flexible CSFs in order to successfully mitigate these vulnerabilities.

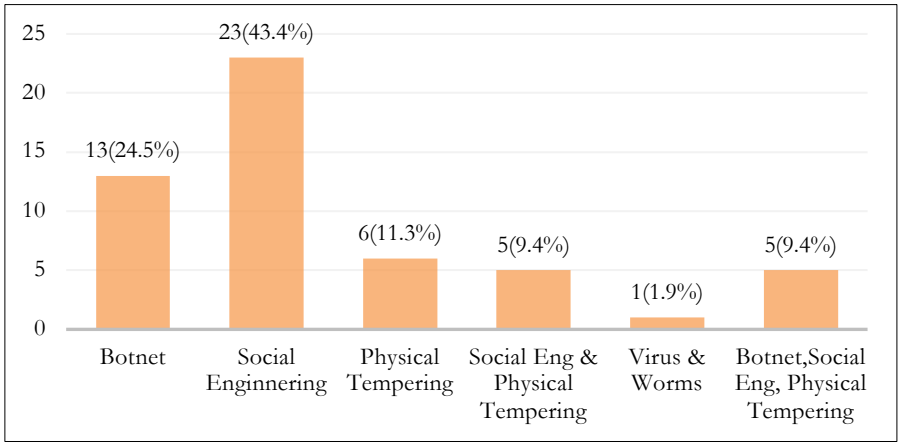

Figure 6. Common Cyber-attacks incidences on IoT devices

Threat identification, detection, asset protection, asset recovery, and threat response are the five essential functions that respondents ranked in order to

assess the performance of the current CSFs. The majority did not rank any of the functions as highly effective, and the mean scores ranged from 2.66 to 2.94 out of a possible 5. Threat identification, for example, received a mean score of 2.74, with 22.6% of respondents indicating that it was insufficient in recognizing all possible dangers. Threat detection had a mean score of 2.72 as well, and none of the respondents thought it was highly successful. According to these views, the current frameworks only provide mediocre threat mitigation, leaving IoT systems vulnerable to possible breaches and undiscovered vulnerabilities.

Table 1. Key Indicators of CSF

Element	Very effective		Effective		Somehow effective		Less effective		Not effective		Mean
	f	%	f	%	f	%	f	%	f	%	
Threat identification	6	11.3	10	18.9	13	24.5	12	22.6	12	22.6	2.74
Threat detection	0	0.0	16	30.2	14	26.4	15	28.3	8	15.1	2.72
Asset protection	6	11.3	14	26.4	9	17.0	18	34.0	6	11.3	2.92
Asset recovery	8	15.1	8	15.1	16	30.2	15	28.3	6	11.3	2.94
Threat response	0	0.0	10	18.9	23	43.4	12	22.6	8	15.1	2.66

According to Table 1's overall findings, the present CSFs are thought to be only moderately effective across all important functions, although providing basic levels of protection and response. Asset protection and recovery, for instance, received scores of 2.92 and 2.94, respectively, suggesting that while some mitigation is there, it is not enough to guarantee complete security or data restoration. Furthermore, threat response scored the lowest at 2.66, indicating inefficiencies and delays in thwarting cyberattacks when they happen. The results are consistent with previous research that highlights the need for comprehensive, responsive, and adaptive CSFs, including those of [35], [36], and [37]. Thus, all of these observations emphasize how vital it is to update and reinforce current CSFs in order to improve the general security of IoT devices.

3.3. Qualitative Analysis through Interviews, Focus Group Discussion, and Documents

Important insights into the organizational and technological difficulties involved in protecting IoT devices using CSFs are provided by the qualitative data gathered through focus groups, interviews, and documentary

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

analysis. Technical vulnerabilities, default configurations, user knowledge, policy dependency, risk management, and ongoing monitoring were among the main themes found in the investigation.

1) Technical Security Challenges in IoT Ecosystems

Technical security flaws in IoT ecosystems, particularly in wired, wireless and hybrid communication devices are shown in Figure 7(i). Unprofessional operation and inadequate protective software, including antivirus, might lead to cyber issues. Expert insights on Figure 7(ii) reveal communication methods intensify vulnerabilities through data interference, unauthorized access and electromagnetic interference (Respondent 1, Field Data 2024). Moreover, real time communication complicates data privacy in sectors like healthcare and the Internet of Medical Things (IoMT) due to interoperability challenges and regulatory constraints [38].

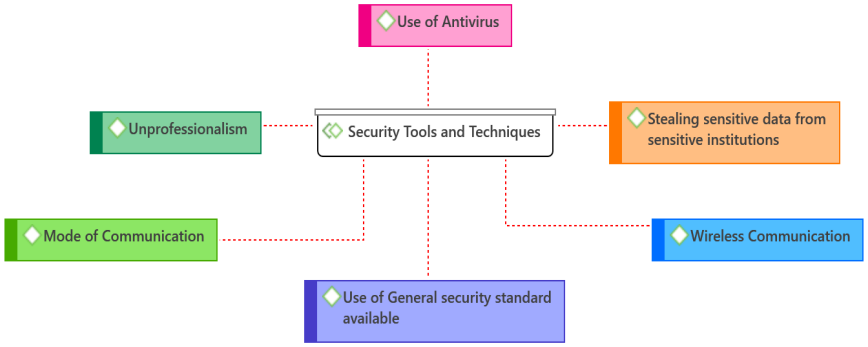

Figure 7 (i). Security Tools and Techniques

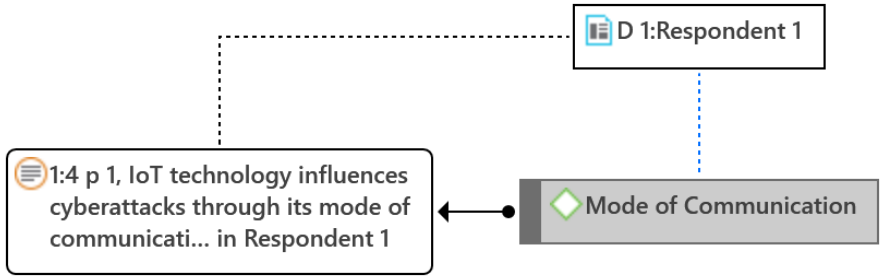

Figure 7 (ii). Technical challenges through the mode of communication

While in agreement to the study findings, [39] confirm that IoT ecosystems exhibit complex vulnerabilities linked to communication protocols and devices interoperability. The study highlights susceptibility to sophisticated

attacks like DoS and man-in-the-middle which increases cyber risks to IoT data due to interoperability deficits and regulatory barriers, paralleling concerns of electromagnetic interference and unauthorized access. Hence, demand for devices security should be adhered to through mode of communication for either wireless or wired and protocols possessed as data exchanged to each other.

2) Default Settings and Patching Vulnerabilities

Respondent 3 attributes data breaches primarily to default device configurations and insufficient patch management (Figure 8). Reliance on basic defenses like firewalls and multifactor authentication leads to underestimated risk exposure [40]. Frequent zero-day exploits and irregular firmware updates compromise system integrity, highlighting the necessity for standardized authentication, encryption, and automated patching under a Zero Trust theory [41].

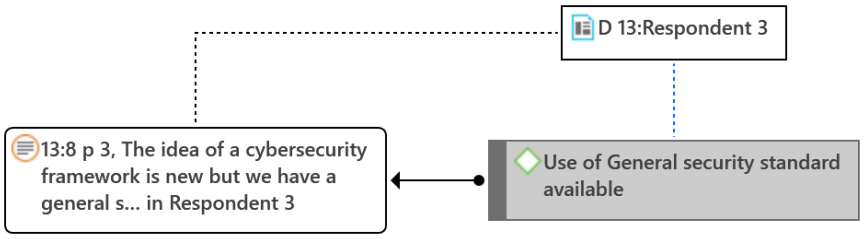

Figure 8. Technical challenges through default settings and patching management

The findings concurs with that in the study by [42] who highlights the shift from perimeter security to Zero Trust (ZT), emphasizing continuous verification of all access requests. In line with protection of IoT devices, it further shows how emerging technologies need ZT through advanced threat detection and real-time decisions. The research also stresses best practices for adopting ZT to address modern cybersecurity challenges like quantum computing and complex attacks.

3) User Awareness and Institutional Policy Gaps

Figure 9 highlights the importance of cybersecurity education for IoT users and ICT administrators, seeing many institutions lack formal CSFs' education, thus rely on internal ICT policies. Regulatory bodies like OSHA and TCRA provide guidance to prevent cyberattacks (Interviewee Y, Field Data 2024). [43] emphasize improvement of information security awareness

in reducing cyber risks, stressing the need for global cybersecurity standards and continuous education for IoT users.

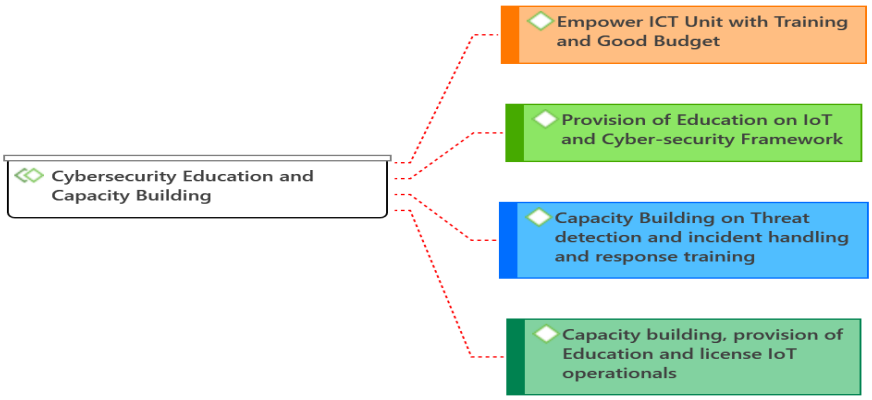

Figure 9. Enhancing Cybersecurity Awareness

The findings resonate positively with the views that Cybersecurity education, empowered ICT units, and effective attack response are vital for strong defenses. Education raises awareness and skills, while a strong ICT team enables timely, resilient responses. Together, they nurture a proactive security culture that reduces vulnerabilities [44]. This integrated approach ensures continuous monitoring, rapid threat detection, and efficient mitigation, enhancing overall organizational resilience against evolving cyber threats. Additionally, ongoing training and resource investment in ICT units foster adaptability and preparedness for emerging challenges in the cybersecurity landscape.

4) Risk Assessment and Cybersecurity Management

In order to maintain fundamental security objectives of confidentiality, integrity, and availability (CIA), risk assessment and management procedures are crucial as shown in Figure 10. There are three ways of evaluating IoT vulnerabilities, reactively, on-demand and scheduled basis (Interviewee J, Field Data, 2024). On-demand assessment is when cyberattacks occur; scheduled assessment is a routine action while reactive assessment is conducted when cyberattacks occur and an examination is required to determine the extent for disaster and its retaliation. Applying traditional risk assessment to modern technologies such as IoT ecosystems is a challenge as new experience and techniques are needed and which involves different areas to be assessed.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

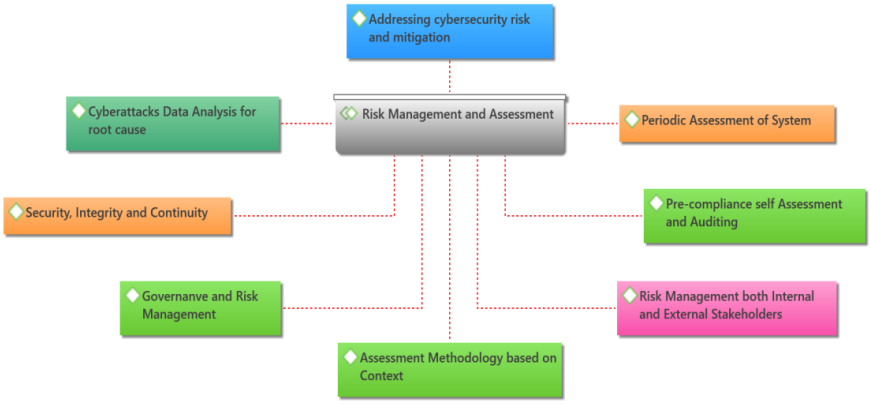

Figure 10. Risk Assessments and Management on IoTs

The study by Affia [45] weighs in by revealing that IoT security risk management (IoT-SRM) framework improves traditional risk management by integrating IoT's layered architecture into security assessments. It splits IoT systems into logical layers to better identify vulnerabilities and interrelated risks. This enables targeted risk discovery and flexible mitigation, offering a more comprehensive approach than reactive or scheduled evaluations alone.

5) Continuous Monitoring and CSF Evaluation

According to the zero-trust theory, which holds that cyberattack incidents are frequently discovered following system underperformance, the group discussion brought to light the lack of structured monitoring systems in many institutions (Group discussion Field Data, 2024). IoT devices have been the target of cyberattacks because of their intricate connectivity to unmonitored systems and devices that lack security framework support. Akinsanya et al. (2024) assert that cyber resilience is improved by ongoing monitoring aided by instruments such as the Assurance Questionnaire (IoTSF, 2021). To protect IoT environments, a Zero Trust strategy is recommended, in which access is constantly checked [46].

In contrast, [47] highlights that many organizations face fragmented monitoring systems, lacking real-time visibility thereby increasing cyber risks. The study recommends automated, continuous monitoring integrated with zero trust principles like dynamic access control and continuous authentication. Also, it supports structured tools similar to the IoTSF Assurance Questionnaire to assess and adapt security, aligning with [48] and [46].

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

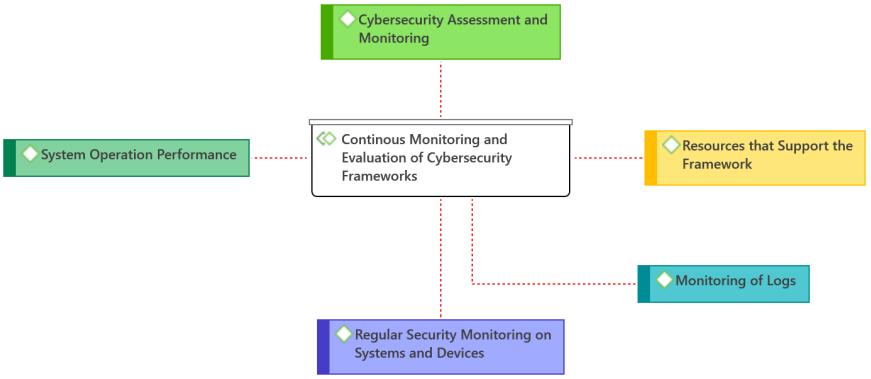

Figure 11. Continuous Monitoring and Evaluation

6) Core features of secure cyber security frameworks for IoT devices

The study found a number of fundamental characteristics that are thought to be necessary for creating a safe cyber security framework for Internet of Things devices as illustrated on Figure 12. A systematic questionnaire was completed by ICT specialists, and the following salient characteristics were validated by theme analysis of qualitative interviews: The NIST Cybersecurity Framework, government security policies, law enforcement, organization ICT policies, safe procurement and disposal of IoT devices, device security standards, cyberattack assessment, data recovery, user education and awareness, and comprehension of IoT devices.

The creation of improved CSFs for IoT devices requires some fundamental security elements, such as adherence to national and international security standards like NIST, which guarantee organized and accepted security procedures [49]. To avoid data interception and unauthorized access during device connection, effective frameworks must incorporate network security protocols and encrypted communication standards such as MQTT, CoAP, and XMPP [50]. For data security and integrity to be maintained across IoT systems, end-to-end encryption is essential [41]. Institutions are held responsible for their cyber security activities through legal enforcement mechanisms that require conformity to cyber security frameworks [43]. It has been determined that reducing human error and inadequate security procedures requires user awareness and technological expertise on the safe usage of devices [40]. Additionally, stronger frameworks need integrated risk assessment and incident management features, such as tools for assessing key performance indicators (KPIs) and conducting cyber audits [45]. Lastly, maintaining interoperability between IoT endpoints facilitates safe

communication and smooth integration across various device ecosystems [48].

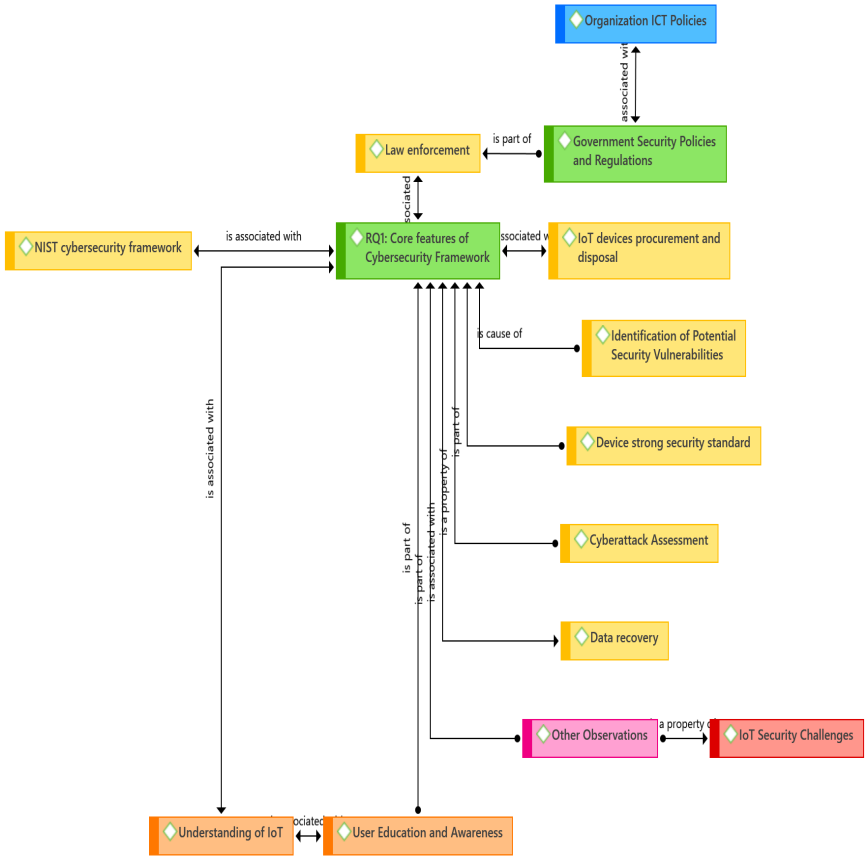

Figure 12. Core Features for Secure Cybersecurity framework

7) Methodologies for Developing IoT Cybersecurity Framework

According to the study, current cyber security frameworks are inadequate to handle new risks posed by cutting-edge technologies like Edge Computing, Artificial Intelligence, and 5G. They are reactive and challenging to assess cyber threats efficiently due to their lack of audit tools, legal enforcement procedures, and predictive capacities [49] [43] [45]. A approach focused on CIA principles, security by design, layered defense, IoT lifecycle management, regulatory compliance, and real-time monitoring is suggested by the study as a means of filling these gaps [48] [41] [50] [40] [46]. In the face of new cyber threats, this integrated approach seeks to guarantee resilience, accountability, and agility.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Analysis indicates that, the creation of Enhanced Cyber Security Framework for IoT devices (ECSF-IoT), must take into account six strategic pillars upon which the framework is based, ranging from the IoT user to the internal security mechanism of the device. In reaction to cyber threats, Zero trust theory operation is needed for device authentication, authorization and continuous security monitoring. Technology acceptance theory is also embraced for new technologies introduced and used on IoT devices though they are coming with different challenges such as emerging cyber-attacks. Significance of developed framework is the enforcement of security responsibilities to IoT device user, manufacturer, and operational processes systems.

The framework integrates user understanding of cyber security and technical expertise on cyber security issues and type of technology IoT device possesses [51]. In order to confirm the efficacy and performance of IoT devices, the framework includes vulnerability assessment and device security auditing. It also allowed IoT users to play a significant role in improving device and data security back to manufacturer of a device. The framework enables users to get assessment results from threat detection and provide security recommendations to manufacturer in the case of security risks or malfunctions.

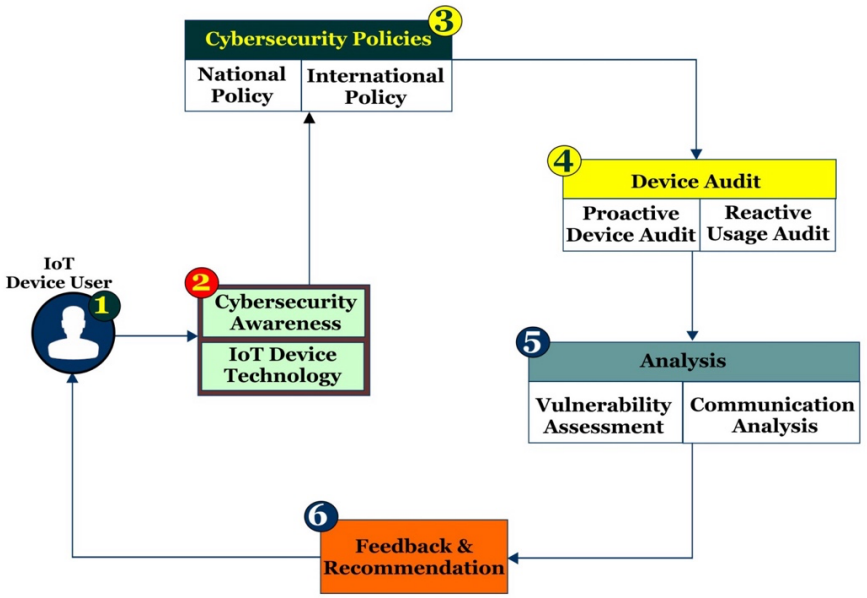

Figure 13. Enhanced Cyber Security Framework for IoT devices (ECSF-IoT)

1. **IoT Device User:** An IoT device user has responsibility for implementing security measures and ensuring compliance with security recommended practices for IoT device. User has responsibility to safeguard the device, for instance, through changing default settings of device and engaging in non-risky behaviors and malpractices [52]. A user also has to provide input to device manufacturers for support needed and improvement of security features to device.
2. i) IoT Device Technology: The technology of IoT device must ensures security is built from the design before taken to the market. Manufacturer has to support IoT user with the software updates and ensure compatibility with other integrated systems as well as new technology trends with its associated cyber risks [53].
   ii) Cybersecurity User awareness: IoT user needs awareness on trending technology and their security risks through provision of security training and best practices for IoT usage. Features such as firmware updates, encryption and network protection against cyber threats has to be understood. Responsibility goes to device management, access controls and continuous security monitoring to reduce vulnerabilities [54]. Awareness on compliance with regulatory standards such as NIST, ISO/IEC 27001 and TCRA ensures devices meet security requirements, protecting against emerging cyber threats.
3. **Cybersecurity Policies:** IoT device can be an entry point for large scale cyber threats and other devices. Technical policies involve the use of encryption standards such as Advanced Encryption Standard (AES) and Transport Layer Security (TLS), secure boot mechanisms, regular firmware updates, network segmentation, and compliance with frameworks like NIST Cybersecurity Framework and ISO/IEC 27001.
   i) National Cybersecurity Policies: Tanzania has developed laws and guidelines that protect people and systems from cybercrime activities these include cybercrime act (2015) and the National ICT policy (2016) [55]. Cyber-crime act include all digital devices and users, any violation may influence cyber-attacks and risk to users' data.
   ii) International Cybersecurity Policies: Adoption of global standards such as NIST Framework promotes risk management and secures system design. Implementation of ISO/IEC 27001 for Information Security Management Systems ensures data are handled securely on IoT device.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

4. **Device Audit:** Audit involve systematic examination for security, device configuration and its performance through identifying vulnerabilities and compliance gaps. By detecting weaknesses on devices earlier, helps to protect sensitive data, prevent unauthorized access and overall security of IoT and systems that facilitates its operation.
   - **i)** Proactive Audit: To secure an organization's data, risk assessment and effective continuous monitoring, as well as strong authentication like Multifactor Authentication and encryption protocols on data both at rest and in transit, as well as changing default settings on devices are necessary. Reconfiguring devices to more securely default options, enforcing diverse encryption protocols, preserving up-to-date software, implementing persistent threat intelligence systems, and employing AI are all methods for enhancing network security [56].
   - **ii)** Reactive Audit and Measures: Incident detection, response and monitoring to mitigate emerging cyber threats through real time alerts and quick action. Device isolation during usage of IoT device to prevent further damage.

5. **Analysis:** This involves evaluating the device's hardware, software and network behavior to identify potential security vulnerabilities.
   - i) Vulnerability Assessment: Scanning and identifying weaknesses such as outdated firmware, open ports or default credentials. It helps to prioritize risks and guides the implementation of security patches and configuration changes.
   - ii) Communication Analysis: Communication or Transport assessment analyses the flow of data and reception through Iot devices and ensure security through their interception or tempering [57]. Protocols such as TLS/SSL to verify for the integrity and confidentiality of transmitted data.

6. **Feedback and Recommendation:** Ongoing cyber security issues, devices usability, challenges or any new vulnerability not captured during initial assessments provide IoT user the way forward for the coming cyber incident challenges. The study [58] agree that continuous improvement and recommendation helps the manufacturer to apply necessary needed security requirements to IoT devices as well as the supply chain management.

3.4. Discussion

The study revealed that although international cybersecurity frameworks like NIST are widely referenced, they are not effectively applied in the Tanzanian context especially to ground users of digital devices. This lack of application is due to poor cybersecurity law enforcement, low user awareness, and the absence of audit tools. Consequently, institutions continue to experience frequent cyberattack incidents, confirming the inadequacy of existing friendly cybersecurity frameworks**.** The identified features such as data encryption, secure protocols, and law compliance, aligning with core security principles of CIA highlighted in global standards of NIST and ISO 27001, confirm a specific comprehensive framework is necessary to enhance IoT security in Tanzania.

Existing literature on IoT cybersecurity highlights the application of established frameworks such as NIST, ISO/IEC 27001, and CIS Controls in managing security risks. However, these frameworks were primarily designed for traditional IT systems and critical infrastructure in well-resourced environments, and they often lack specific provisions for the unique challenges of IoT ecosystems [35]. Issues such as device heterogeneity, limited computational capacity, and inadequate user awareness are frequently overlooked, making implementation ineffective in practice [59]. This suggests that while these frameworks offer many guidelines, they may not fully address contextual limitations in resource-constrained environments.

In contrast, the proposed framework in this study is in focus to the specific needs and infrastructural realities of IoT usage in Tanzania. Unlike generalized models, it integrates localized threat assessments and prioritizes practical, low-cost security measures suitable for developing features. This approach offers a more feasible path toward improving IoT security compared to traditional models that assume broader technological and institutional capacities [60]. Therefore, this research contributes a contextualized alternative to existing global frameworks.

This study proposes a localized cybersecurity framework for Tanzanian institutions, addressing a critical gap in existing approaches by integrating both technical measures and human-centric factors such as regulatory enforcement and user awareness. While previous efforts, including national strategies and global guidelines, aimed to control cybercrime, institutions in Tanzania still face increasing threats due to widespread use of unsecured imported IoT devices and insufficient cybersecurity awareness [61] [15] [14]. The growing scale of IoT device adoption is projected to reach $6 trillion

globally by 2025 which further complicates the threat landscape [62]. Despite national efforts like the Tanzania National Cyber Security Strategy (2022–2027), sectors such as health, finance, and education remain vulnerable due to evolving cybercriminal tactics that exploit advanced technologies like AI, IoT, and cloud computing [17] [18]. This research fills a gap in literature by developing a cybersecurity framework that emphasizes enforceable local policies, continuous awareness programs, and measurable compliance tools to strengthen institutional resilience against emerging cyber threats [63].

The study faced several limitations that impacted its scope and efficiency, such as limited time of participants to cooperate on study discussion and their expertise inputs which caused data collection to be delayed. Additionally, identifying and getting cybersecurity experts proved challenging. The geographic scope and sample size were further constrained by the cost of accessing various places within the study area. Technological constraints were also evident, particularly in capturing clear and accurate audio recordings during interviews and group discussions, which may have affected data quality and transcription accuracy. Lastly, delays in participant responses to Google Form questionnaires prolonged the time needed to collect all the data, slowed down the study's progress.

Despite the limitations faced in the study, several solutions helped mitigating these challenges: researcher requested flexible scheduling and timely reminders to improve participant availability. Expanding networks through ICT professional associations from Tanzania Universities, and government agencies related to cyber issues and online platforms to access more cybersecurity experts. On the overcoming audio capturing, the researcher used virtual methods like video calls to reduce travel costs, employing reliable, high-quality recording equipment to enhance audio capture; and sending messages to remind respondents to speed up questionnaire responses.

4. CONCLUSION

This study concludes based on the findings that the security for Internet of Things (IoT) devices in Tanzania remains a critical concern due to the widespread use of unsecured and low-standard imported digital devices, evolving cyber threats, and insufficient cybersecurity awareness. Despite the presence of national strategies and international cybersecurity frameworks, many Tanzanian institutions continue to report persistent cybercrime cases, particularly in sensitive sectors like health, education, and finance. The growing integration of IoT devices with advanced technologies like cloud

computing and artificial intelligence further complicates the threat landscape, necessitating more responsive and localized security strategies. The development of Enhanced Cybersecurity Framework for IoT device (ECSF-IoT) represents a significant step toward addressing these complex challenges by combining both technical controls and human-centric components. The framework emphasize on enforced cybersecurity policies, continuous awareness programs and auditable metrics supports institutional commitment to reducing attack surfaces and promoting safe IoT practices.

For effective implementation, policymakers must focus on strengthening localized regulations that mandate minimum security standards for IoT devices entering the Tanzanian market, particularly those imported with low security features. IoT device manufacturers should collaborate closely with government agencies such as Tanzania Communication Regulatory Authority (TCRA), Tanzania Police Force and cybersecurity experts to embed security by design principles towards local threat vectors. As a next step, pilot projects involving public and private institutions in sectors vulnerable to cyber threats such as healthcare, finance and national security should be launched to test the framework's applicability and international bodies can facilitate knowledge transfer and co-development of practical security solutions. Continuous monitoring and feedback from these pilots will guide iterative improvements of ECSF-IoT ensuring its adaptability and sustainability in Tanzania's evolving digital ecosystem.

REFERENCES

[1] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," *Mob. Netw. Appl.*, vol. 28, no. 1, pp. 296–312, Feb. 2023, doi: 10.1007/s11036-022-01937-3.

[2] K. S. Mohamed, "An Introduction to IoT," in *Bluetooth 5.0 Modem Design for IoT Devices*, Cham: Springer International Publishing, 2022, pp. 33–43. doi: 10.1007/978-3-030-88626-4_2.

[3] J. C. Talwana and H. J. Hua, "Smart World of Internet of Things (IoT) and Its Security Concerns," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Dec. 2016, pp. 240–245. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.64.

[4] V. M. Kuthadi, R. Selvaraj, Y. V. Rao, P. S. Kumar, M. Mustafa, K. Phasinam, and E. Okoronkwo, "Towards security and privacy concerns in the internet of things in the agriculture sector," *Turk. J. Physiother. Rehabil.*, vol. 32, no. 3, pp. 1–12, 2023.

[5] M. Ahmid and O. Kazar, "A Comprehensive Review of the Internet of Things Security," *J. Appl. Secur. Res.*, vol. 18, no. 3, pp. 289–305, Jul. 2023, doi: 10.1080/19361610.2021.1962677.

[6] A. D. Khaleefah and H. M. Al-Mashhadi, "Methodologies, requirements, and challenges of cybersecurity frameworks: a review," *Iraqi J. Sci.*, vol. 65, no. 1, pp. 468–486, Jan. 2024, doi: 10.24996/ijs.2024.65.1.38.

[7] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models," *Sensors*, vol. 22, no. 9, Art. no. 9, Jan. 2022, doi: 10.3390/s22093367.

[8] F. Mwamba and E. A. Mjema, "The Effects of Phishing Attacks on Mobile Phone Users in Tanzania: A Case of Kariakoo Market, Dar es Salaam," *Afr. J. Empir. Res.*, vol. 5, no. 4, Art. no. 4, Nov. 2024.

[9] G. N. Noah, "Examining security awareness level on emerging internet of things (IoT) usage to the end user in Arusha, Tanzania," Ph.D. dissertation, Inst. of Accountancy Arusha, Tanzania, 2022.

[10] E. Mkilia, J. T. Kaleshu, and A. S. Sife, "Cybersecurity Risks and Customers' Protective Behavior on Usage of Mobile Banking Services: Evidence from Selected Banks in Tanzania," *Local Adm. J.*, vol. 16, no. 3, Art. no. 3, Sep. 2023.

[11] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, Art. no. 14, Jan. 2022, doi: 10.3390/electronics11142181.

[12] A. B. Feroz Khan, M. M. Hussain, S. Kalpana Devi, and M. A. Gunavathie, "DDoS attack modeling and resistance using trust based protocol for the security of Internet of Things," *J. Eng. Res.*, vol. 11, no. 2, p. 100058, Jun. 2023, doi: 10.1016/j.jer.2023.100058.

[13] M. Fagan, K. N. Megas, K. Scarfone, and M. Smith, "IoT device cybersecurity capability core baseline," National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8259A, May 2020. doi: 10.6028/NIST.IR.8259a.

[14] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Secur. Appl.*, vol. 2, p. 100031, Jan. 2024, doi: 10.1016/j.csa.2023.100031.

[15] P. Bastos, L. Castro, and M. Cruz, *The Quality and Price of Africa's Imports of Digital Goods*. in Policy Research Working Papers. The World Bank, 2024. doi: 10.1596/1813-9450-10718.

[16] P. C. Mbwana, "The Legal Disruption of Cybercrime in Tanzania: A Social-Economic Analysis," Oct. 09, 2023, *Social Science Research Network, Rochester, NY*: 4596873. doi: 10.2139/ssrn.4596873.

[17] H. Pallangyo, "Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services," *Tanzan. J. Eng. Technol.*, vol. 41, no. 2, pp. 189–204, Aug. 2022, doi: 10.52339/tjet.v41i2.792.

[18] M. Thakur, "Cyber Security Threats and Countermeasures in Digital Age," *J. Appl. Sci. Educ. JASE*, vol. 4, no. 1, Art. no. 1, Apr. 2024, doi: 10.54060/a2zjournals.jase.42.

[19] M. Fagan, J. Marron, K. Brady, B. Cuthill, K. Megas, and R. Herold, "Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline," National Institute of Standards and Technology, NIST Internal or Interagency Report (NISTIR) 8259C (Draft), Dec. 2020. doi: 10.6028/NIST.IR.8259C-draft.

[20] M. Burhan *et al.*, "A Comprehensive Survey on the Cooperation of Fog Computing Paradigm-Based IoT Applications: Layered Architecture, Real-Time Security Issues, and Solutions," *IEEE Access*, vol. 11, pp. 73303–73329, 2023, doi: 10.1109/ACCESS.2023.3294479.

[21] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors*, vol. 23, no. 8, Art. no. 8, Jan. 2023, doi: 10.3390/s23084117.

[22] N. Kshetri, "Cybercrime and Cybersecurity in Africa," *J. Glob. Inf. Technol. Manag.*, vol. 22, no. 2, pp. 77–81, Apr. 2019, doi: 10.1080/1097198X.2019.1603527.

[23] N. F. Khan, N. Ikram, S. Saleem, and S. Zafar, "Cyber-security and risky behaviors in a developing country context: a Pakistani perspective," *Secur. J.*, pp. 1–33, May 2022, doi: 10.1057/s41284-022-00343-4.

[24] D. Nagpal, I. Kornerup, and M. P. Gibson, "Mixed-method Research: A Basic Understanding," *CODS J. Dent.*, vol. 12, no. 1, pp. 11–16, Apr. 2021, doi: 10.5005/jp-journals-10063-0065.

[25] A. N. Masawe and D. B. Ally, "Effectiveness of Cybersecurity Awareness Training on Mitigating Insider Threat: The Case of Arusha Airport," *Afr. Conf. Appl. Inform.*, Dec. 2024, doi: 10.59645/acai.v4i1.328.

[26] Y. Su and M. Li, "Applying Technology Acceptance Model in Online Entrepreneurship Education for New Entrepreneurs," *Front. Psychol.*, vol. 12, p. 713239, Oct. 2021, doi: 10.3389/fpsyg.2021.713239.

[27] M. H. Kalayou, B. F. Endehabtu, and B. Tilahun, "The Applicability of the Modified Technology Acceptance Model (TAM) on the Sustainable Adoption of eHealth Systems in Resource-Limited Settings," *J. Multidiscip. Healthc.*, vol. Volume 13, pp. 1827–1837, Dec. 2020, doi: 10.2147/JMDH.S284973.

[28] P. Gill and J. Baillie, "Interviews and focus groups in qualitative research: an update for the digital age," *Br. Dent. J.*, vol. 225, no. 7, pp. 668–672, Oct. 2018, doi: 10.1038/sj.bdj.2018.815.

[29] T. S. Jalolov, "Use of SPSS Software in Psychological Data Analysis," *Psixologiya Va Sotsiologiya Ilmiy Jurnali*, vol. 2, no. 7, Art. no. 7, Aug. 2024.

[30] U. N. Sharma, "Basic Stages of Analyzing Qualitative Documents Using ATLAS.ti," *Access Int. J. Nepal Libr. Assoc.*, vol. 3, pp. 112–132, Sep. 2024, doi: 10.3126/access.v3i1.69427.

[31] D. Lakens, "Sample Size Justification," *Collabra Psychol.*, vol. 8, no. 1, p. 33267, Mar. 2022, doi: 10.1525/collabra.33267.

[32] Bostley Muyembe Asenahabi and Peters Anselemo Ikoha, "Scientific Research Sample Size Determination," *Int. J. Sci. Technoledge*, Aug. 2023, doi: 10.24940/theijst/2023/v11/i7/ST2307-008.

[33] M. Marcel and N. C. Azhar, "Contextual ITSM Adoption Across Educational Levels: A University and a Secondary School in Jakarta," *J. Inf. Syst. Inform.*, vol. 7, no. 2, pp. 1105–1147, Jun. 2025, doi: 10.51519/journalisi.v7i2.1081.

[34] C. A. Wong *et al.*, "Strategies for research participant engagement: A synthetic review and conceptual framework," *Clin. Trials*, vol. 18, no. 4, pp. 457–465, Aug. 2021, doi: 10.1177/17407745211011068.

[35] A. D. Khaleefah and H. M. Al-Mashhadi, "Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review," *Iraqi J. Sci.*, pp. 468–486, Jan. 2024, doi: 10.24996/ijs.2024.65.1.38.

[36] R. H. Chowdhury, N. U. Prince, S. M. Abdullah, and L. A. Mim, "The role of predictive analytics in cybersecurity: detecting and preventing threats," *World J. Adv. Res. Rev.*, vol. 23, no. 2, pp. 1615–1623, Feb. 2024, doi: 10.30574/wjarr.2024.23.2.2494.

[37] T. Vassiliadis and J. Hedström, *The challenges and opportunities in incident response for companies*. 2024. Accessed: Sep. 30, 2024. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-24067

[38] J. Mulo *et al.*, "Navigating Challenges and Harnessing Opportunities: Deep Learning Applications in Internet of Medical Things," *Future Internet*, vol. 17, no. 3, Art. no. 3, Mar. 2025, doi: 10.3390/fi17030107.

[39] V. R. Konduru and M. R. Bharamagoudra, "Challenges and solutions of interoperability on IoT: How far have we come in resolving the IoT interoperability issues," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Aug. 2017, pp. 572–576. doi: 10.1109/SmartTechCon.2017.8358436.

[40] S. Madnick, "Why data breaches spiked in 2023," *Harvard Business Review*, Feb. 2024. [Online]. Available: https://hbr.org/2024/02/why-data-breaches-spiked-in-2023

[41] S. El Jaouhari and E. Bouvet, "Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions," *Internet Things*, vol. 18, p. 100508, May 2022, doi: 10.1016/j.iot.2022.100508.

[42] A. I. Weinberg and K. Cohen, "Zero Trust Implementation in the Emerging Technologies Era: Survey," Jan. 17, 2024, *arXiv*: arXiv:2401.09575. doi: 10.48550/arXiv.2401.09575.

[43] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, Mar. 2023, doi: 10.1016/j.heliyon.2023.e14234.

[44] E. Stavrou and A. Piki, "Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity," *Inf. Comput. Secur.*, vol. 32, no. 4, pp. 523–541, Jul. 2024, doi: 10.1108/ICS-02-2024-0038.

[45] A. O. Affia, A. Nolte, and R. Matulevičius, "IoT Security Risk Management: A Framework and Teaching Approach," *Inform. Educ.*, Apr. 2023, doi: 10.15388/infedu.2023.30.

[46] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," *Internet Things*, vol. 27, p. 101227, Oct. 2024, doi: 10.1016/j.iot.2024.101227.

[47] M. Sayed, "The Internet of Things (IoT), Applications and Challenges: A Comprehensive Review," *J. Innov. Intell. Comput. Emerg. Technol. JIICET*, vol. 1, no. 01, pp. 20–27, Jan. 2024.

[48] M. O. Akinsanya, C. C. Ekechi, and C. D. Okeke, "The Evolution of Cyber Resilience Frameworks in Network Security: A Conceptual Analysis," *Comput. Sci. IT Res. J.*, vol. 5, no. 4, Art. no. 4, Apr. 2024, doi: 10.51594/csitrj.v5i4.1081.

[49] T. S. AlSalem, M. A. Almaiah, and A. Lutfi, "Cybersecurity Risk Analysis in the IoT: A Systematic Review," *Electronics*, vol. 12, no. 18, Art. no. 18, Jan. 2023, doi: 10.3390/electronics12183958.

[50] Ł. Lemieszewski, D. Hannebauer, and G. Remiszewski, "Vulnerability of Wi-Fi wireless network to signal interference," *J. Eng. 360 JoE 360*, vol. 1, no. 1/24, pp. 58–65, 2024.

[51] A. A. Maqousi, "A Proposed Framework for User Cybersecurity Awareness," in *2023 24th International Arab Conference on Information Technology (ACIT)*, Dec. 2023, pp. 1–6. doi: 10.1109/ACIT58888.2023.10453904.

[52] J. Ye, X. D. C. De Carnavalet, L. Zhao, M. Zhang, L. Wu, and W. Zhang, "Exposed by Default: A Security Analysis of Home Router Default Settings," in *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, in ASIA CCS '24. New York, NY, USA: Association for Computing Machinery, Jul. 2024, pp. 63–79. doi: 10.1145/3634737.3637671.

[53] C. Sisavath and L. Yu, "Design and implementation of security system for smart home based on IOT technology," *Procedia Comput. Sci.*, vol. 183, pp. 4–13, Jan. 2021, doi: 10.1016/j.procs.2021.02.023.

[54] K. Ragothaman, Y. Wang, B. Rimal, and M. Lawrence, "Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions," *Sensors*, vol. 23, no. 4, Art. no. 4, Jan. 2023, doi: 10.3390/s23041805.

[55] N. S. Shalua and A. A. Semlambo, "Strengthening Tanzania's Digital Infrastructure: Assessing Cyber Threats to the Government e-Payment Gateway for National Security," vol. 6, no. 4.

[56] H. Wu, H. Han, X. Wang, and S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, pp. 153826–153848, 2020, doi: 10.1109/ACCESS.2020.3018170.

[57] A. L. Canino and G. Lax, "Enabling Lawful Interception in Environments Protected by IoT Safeguard," in *Electronic Government and the Information Systems Perspective*, A. Kö, G. Kotsis, A. M. Tjoa, and I. Khalil, Eds., Cham: Springer Nature Switzerland, 2024, pp. 139–153. doi: 10.1007/978-3-031-68211-7_12.

[58] K. Sallam, M. Mohamed, and A. W. Mohamed, "Internet of Things (IoT) in Supply Chain Management: Challenges, Opportunities, and Best Practices," *Sustain. Mach. Intell. J.*, vol. 2, pp. 1-32, Mar. 2023, doi: 10.61185/SMIJ.2023.22103.

[59] M. Noaman, M. S. Khan, M. F. Abrar, S. Ali, A. Alvi, and M. A. Saleem, "Challenges in integration of heterogeneous internet of things," *Sci. Program.*, vol. 2022, Art. no. 8626882, pp. 1–15, 2022, doi: 10.1155/2022/8626882.

[60] J. Nyansiro, J. Mtebe, and M. Kissaka, "A Goal-Oriented Requirements Engineering Framework for E-government Information Systems," *East Afr. J. Sci. Technol. Innov.*, vol. 2, no. 4, Art. no. 4, Sep. 2021, doi: 10.37425/eajsti.v2i4.283.

[61] B. Mtakati and F. Sengati, "Cybersecurity Posture of Higher Learning Institutions in Tanzania," *J. Inform.*, vol. 1, no. 1, Mar. 2021, doi: 10.59645/tji.v1i1.1.

[62] J. Shehu Yalli, M. Hilmi Hasan, and A. Abubakar Badawi, "Internet of Things (IoT): Origins, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade," *IEEE Access*, vol. 12, pp. 91357–91382, 2024, doi: 10.1109/ACCESS.2024.3418995.

[63] N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," *Sensors*, vol. 25, no. 1, Art. no. 1, Jan. 2025, doi: 10.3390/s25010079.