Internet of Things (IoT) Security: Risk Assessment and Management Models

Osanaiye, O. A.[1,*], Odimba, U.[2], Ogundile, O. O.[3]
[1,*] Department of Mechatronics Engineering, Nile University of Nigeria, Abuja, Nigeria
[2]Africa Centre of Excellence on Technology Enhanced Learning, National Open University of Nigeria, Abuja, Nigeria
[3]Department of Computer Science, Tai Solarin University of Education, Ijebu Ode, Ogun State, Nigeria
[*]Corresponding author: opeyemi.osanaiye@nileuniversity.edu.ng

ABSTRACT: Today, machines, appliances, homes, offices, vehicles, sensors, and systems across many sectors of human endeavours can be interconnected to exchange information and autonomously perform tasks. All these efforts are geared toward creating a smarter society. These have ushered in a new era in the technological landscape of devices on the Internet through multiple networks known as the Internet of Things (IoT). The swift expansion of the Internet of Things (IoT) has dramatically transformed numerous sectors by interlinking devices and facilitating smooth data sharing. Yet, this enhanced interconnectedness also bring about substantial cybersecurity challenges. With the continuous expansion of the Internet of Things (IoT), it is essential to have robust risk assessment and management in place to mitigate cybersecurity risks. Currently, there is no general IoT security model and efforts to standardize IoT security are at their infantry phase. There are only a few IoT security standards, and best practices are not focused on IoT security risk assessment and management. This paper reviews some existing risk assessment and management models for IoT and proposes innovative improvements to address identified gaps. The proposed model strives to fortify IoT systems, ensuring their reliability, security, and efficient performance. By evaluating the strengths and weaknesses of current models and embracing improved models, organizations can better assess and manage risks associated with IoT deployments.

KEYWORDS: Internet of Things (IoT), Cybersecurity, Risk assessment, Risk management, IoT-specific challenges

1. INTRODUCTION

The world is rapidly advancing in automation. Continuing progression in computing technologies such as the Internet, communication networks, information systems, and smart devices has further given rise to more opportunities for automation and interconnectedness. Today, machines, appliances, homes, offices, vehicles, sensors, and systems across many sectors of human endeavours can be interconnected to exchange information autonomously to perform tasks simultaneously, and be remotely controllable. All these efforts are geared toward creating a smarter society.

These developments have ushered in a new era in the technological landscape of devices on the Internet through multiple networks known as the Internet of Things (IoT). IoT is ubiquitous and has been applied in aspects of existence and fields such as automobiles, transportation, smart homes, smart cities, energy supply, health care delivery, industrial processes, and supply chain management, among others. IoT devices result from the convergence of information technology (IT) and operational technology (OT) (NIST, 2018).

The global count of Internet of Things (IoT) devices has seen a consistent upward trend in the past few years. Studies have shown that IoT has immense potential economic value which is large and growing. It is estimated that by 2030, the IoT could enable $5.5 trillion to $12.6 trillion in value globally, including the value captured by consumers and customers of IoT products and services (Michael Chui et. al., 2021).

While the emergence and the continuing growth of IoT have opened a new vista of opportunities in terms of improving the quality of life as well as creating vast economic opportunities, it has also come along with enormous risks (Meneghello et. al., 2019). The fact that the number of IoT devices is growing at exponential rates and its adoption is expanding further into many fields means there is much to worry about in the coming decades regarding the threats and risks posed by IoT.

How can these interconnected systems and devices be protected from the threats of attacks? This brings us to the concept of the cybersecurity of IoT. Cybersecurity is the collection of policies, techniques, technologies, and processes that work together to protect the confidentiality, integrity, and availability of computing resources, networks, software programs, and data from attack (Berman et. al., 2019).

Already, there are troubling statistics about malware attacks on existing IoT devices and systems. In recent years, there have been high-profile breaches of critical systems running on IoT. According to Kaspersky, some 1.51 billion IoT breaches occurred from January to June 2021 (Cyrus, 2021).

Considering the data privacy concerns and cybersecurity implications of IoT, several studies have been conducted in this emerging field of IoT against attendant threats and vulnerabilities (Osanaiye et al, 2022). Similarly, studies have been carried out on risk assessment models and cybersecurity in information systems in general (Dhillon, 2016). However, studies on the application of risk management principles to assess and mitigate these risks associated with IoT seem rare based on reviews carried out so far.

According to McKinsey & Company, there is no general IoT security model. Similarly, efforts to standardize IoT security still seem to be at their infantry phase. There are only a few IoT security standards, and best practices are not focused on IoT security risk assessment and management (Popescu et. al., 2021). Considering this clear research gap in terms of the existence of an IoT security risk assessment and management strategy reference model, thus a need for this research work.

The goals of risk management are to identify, measure, control, and minimize the losses associated with uncertain events or risks. Risk assessment includes tasks such as analyzing assets, identifying vulnerabilities and potential risks due to threats, finding risk-reducing measures, and making decisions related to the acceptance, avoidance, or transfer of risk (Kau and Lashkari, 2021). Risk management also includes determining risk-reducing measures and budgeting, implementing, maintaining, and having priorities assigned to the measures.

Having shown the benefits and growing application of IoT and the enormous implications that can occur when such a system is compromised or breached, then the questions arise: What are the potential risks with IoT and how can these risks be assessed and effectively managed? This paper reviews existing risk assessment and management models for IoT and proposes improvements or a new model for enhanced effectiveness. By evaluating the strengths and weaknesses of current models, and incorporating IoT's unique challenges, organizations can better assess and manage risks associated with IoT deployments.

2. RELATED WORKS

The risk assessment and management approaches in cybersecurity that have been extended to IoTs will be explored. Furthermore, we will provide an examination of the relevant studies on this risk assessment method that contributes to simplifying the task of maintaining security conditions.

Model 1: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk-based strategic assessment and planning technique for security. The model was developed by the Software Engineering Institute (SEI) at Carnegie Mellon University (Hashim et. al., 2018). OCTAVE is not specific to IoT but is commonly applied in various technological contexts, including IoT (Radanliev et. al., 2018).

The OCTAVE model (Figure 1) has some strengths which make it a veritable model for assessing and managing risks in systems. For example, OCTAVE takes a holistic approach, considering all elements within an organization that may contribute to risk. This includes not only technology but also people and operational processes. Also, OCTAVE is designed to be a self-directed method. This means that organizations can implement OCTAVE using their staff, which increases internal awareness and understanding of the organization's risks and vulnerabilities. Although it is not a one-size-fits-all model, it is a framework that organizations can adapt to their specific needs, contexts, and resources.

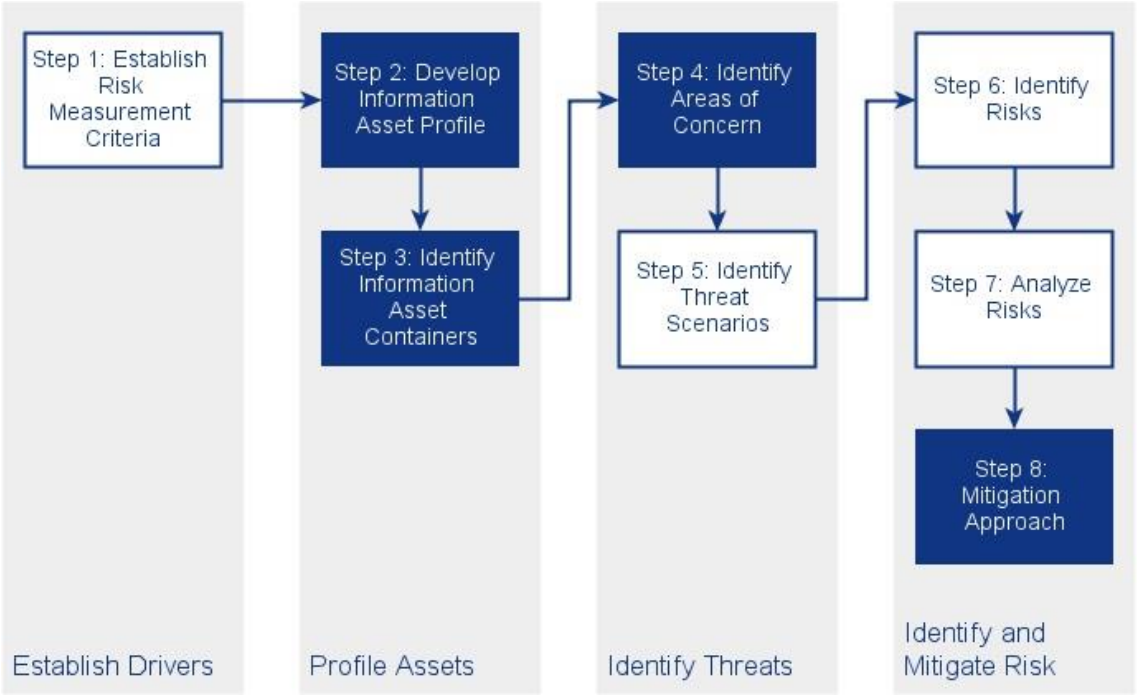

Fig. 1: The OCTAVE Model (sunflower-cissp, 2019)

However, OCTAVE has its challenges and areas for improvement. As a comprehensive and participatory process, OCTAVE can be time and resource-intensive. For organizations with limited resources or urgent security needs, this could be a significant challenge (Alshboul and Streff, 2015). Additionally, while OCTAVE is self-directed, it requires a reasonable level of expertise to execute effectively. Without sufficient in-house knowledge and skill,

organizations may struggle to implement the model effectively. OCTAVE is versatile and can be applied to various contexts, yet it does not specifically address the unique challenges of IoT. As such, organizations may need to augment OCTAVE with additional tools or strategies tailored to IoT security.

Model 2: NIST SP 800-30 Risk Management Framework

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 is a framework for conducting risk assessments. It is part of the broader NIST Risk Management Framework (RMF) that provides a structured process for integrating security and risk management activities into the system development lifecycle. The main advantage of the NIST SP 800-30 is that it is part of a wider, more comprehensive risk management framework. It outlines detailed steps for risk assessment, including preparing for the assessment, conducting it, communicating the results, and maintaining the assessment (NIST, 2012). Similarly, as a NIST publication, it comes with a high level of credibility and is widely accepted in various industries. The NIST (RMF), including SP 800-30, is used to provide risk assessment guidelines for government agencies and private sector organizations (Al Fikri et. al., 2019). The NIST SP 800-30 is accompanied by thorough documentation, providing detailed guidance for organizations conducting risk assessments. This helps ensure the process is both comprehensive and transparent.

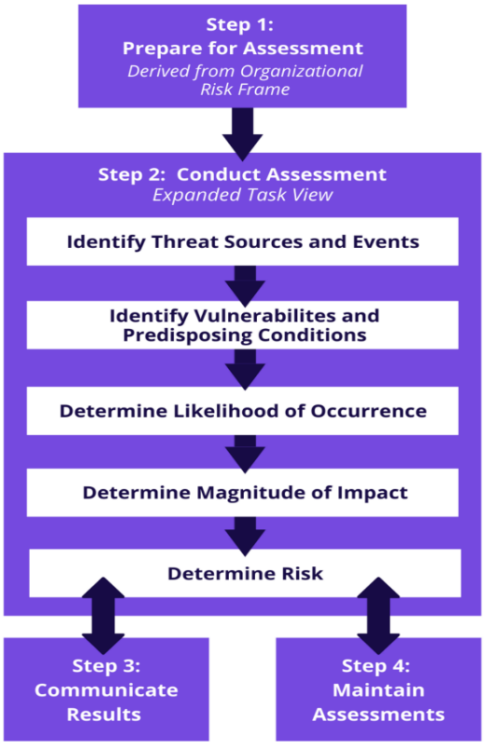

Fig. 2: NIST SP 800-30 Risk Management Framework (Cyvatar, 2021)

On the other hand, the NIST SP 800-30 framework (Figure 2) is not without its drawbacks. It can be quite complex, especially for organizations without much experience in risk assessment. It requires a certain level of expertise to implement effectively. Furthermore, due to its comprehensive nature, implementing NIST SP 800-30 can be resource-intensive, potentially posing a challenge for organizations with limited resources. Like many general risk

assessment frameworks, NIST SP 800-30 is high-level and does not specifically address the unique challenges and risks associated with IoT. As a result, it may need to be supplemented with additional IoT-specific risk assessment strategies.

The NIST SP 800-30 is a credible and comprehensive guide for conducting risk assessments. However, organizations looking to apply it to IoT environments may need to supplement it with additional strategies to address the unique risks and challenges associated with IoT.

Model 3: ISO/IEC 27005 Information Security Risk Management

ISO/IEC 27005 is a standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that provides guidelines for information security risk management. One benefit of the ISO/IEC 27005 model is that it offers a comprehensive framework for managing information security risks, including the entire process from risk assessment to risk treatment (Wangen et. al., 2018). As part of the ISO 27000 series, this standard aligns well with other ISO information security standards (Al Fikria, 2019). This can help organizations achieve a more cohesive and integrated approach to information security. The ISO/IEC standards are globally recognized and respected, and compliance with these standards can enhance an organization's credibility.

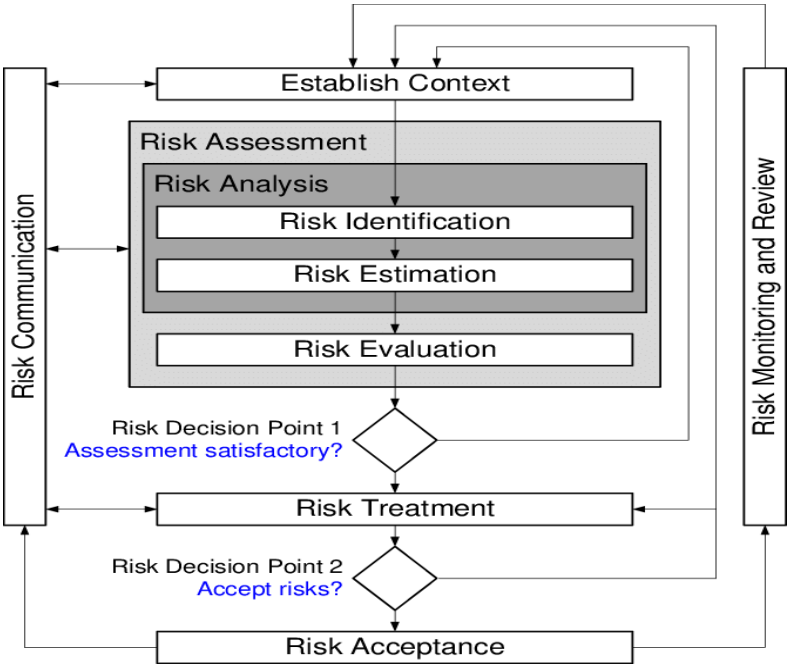

Fig. 3: ISO/IEC 27005 (ISO, 2011)

ISO/IEC 27005 is a general information security standard and thus, does not specifically address the unique challenges and risks associated with IoT. Thus, organizations may need to supplement it with additional IoT-specific risk assessment and management strategies. Another challenge with SO/IEC 27005 is that it can be complex to implement, particularly for organizations without a solid background in information security risk management. The standard may require considerable time and resources to fully implement. Implementing ISO standards, including ISO/IEC 27005, can be costly. The cost includes not only the cost of the standard itself but

also the resources required for implementation, potential consulting fees, and the cost of certification if the organization chooses to become certified.

ISO/IEC 27005 (Figure 3) is a globally recognized and comprehensive standard for information security risk management (Patiño et. al., 2018). However, organizations looking to apply it in an IoT context may need to address additional challenges and risks specific to IoT environments. As with any standard or framework, successful implementation requires a commitment of resources and organizational support.

Model 4: Factor Analysis of Information Risk (FAIR)

Factor Analysis of Information Risk (FAIR) is a risk analysis model and framework (Figure 4) that provides a standard taxonomy and ontology for evaluating and quantifying information risk in a way that is both practical and grounded in economic principles (Whitman and Mattord, 2013). It helps organizations understand, analyze, and quantify information risk in financial terms (Fair Institute, 2022).

FAIR uses the quantitative approach in assessing and managing risks (Radanliev, 2018). Unlike many other risk assessment models, FAIR aims to quantify risk in financial terms. This can make it easier and more attractive for businesses to incorporate risk assessment into their decision-making processes. Likewise, it provides a standardized language for discussing and understanding risk. This can help to break down silos within an organization, improving communication around risk. Another strength of FAIR is its focus on probabilities. It looks at risk in terms of probabilities and impact, which can help organizations develop a more nuanced understanding of their risk landscape (The Open Group, 2009).

Fig. 4: FAIR Model (Fair Institute, 2022)

Despite its strengths, FAIR also has its shortcomings (Balbix. 2022). To implement FAIR effectively, an organization may require a certain level of expertise. Without this expertise, there is a risk that the model could be applied incorrectly. Like other current risk assessment and management models, FAIR is not specifically designed for IoT environments, and while it can be adapted for such use, it may not capture all the unique aspects

of IoT risk. Again, quantifying risk in the way FAIR recommends can be time-consuming and resource-intensive. While it can ultimately lead to more effective risk management, the upfront investment required may be a barrier for some organizations.

FAIR offers a unique approach to risk management with its focus on quantification and probabilities. However, organizations need to be aware of the resources and expertise required to effectively implement the model, and additional considerations may be necessary for IoT-specific risks.

Model 5: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE)

STRIDE is a threat modeling methodology developed by Loren Kohnfelder and Praerit Garg in 1999. It was adopted by Microsoft and incorporated into its structure in 2002 (Saikat Das et. al., 2021). STRIDE is a model for finding threats in a system being designed or existing. The acronym STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. These are the categories of threats that the methodology aims to identify and mitigate.

One major strength of STRIDE is that it offers comprehensive categorization (Viswanathan and Jayagopal, 2021). STRIDE (Figure 5) provides a broad categorization of threats, which can be a useful tool for ensuring that an organization considers a wide range of potential security issues. Moreover, when compared to some other threat modeling methodologies. STRIDE was developed by Microsoft, a well-known and trusted entity in the world of technology, and it is relatively simple and easy to use, making it accessible to a wide range of organizations (Kim et. al., 2022).

Fig. 5: STRIDE Model (Defense Lead. 2021)

Conversely, there are some challenges and areas that require improvement in the model. STRIDE is designed to identify threats, not to assess risks. This means it does not prioritize threats based on their potential impact or likelihood. As such, organizations may need to complement STRIDE with a risk-based approach to effectively manage their security. Again, like many other threat modeling methodologies, STRIDE is not specifically designed for IoT environments. While it can certainly be used in an IoT context, it may not capture all the unique aspects of IoT security. Furthermore, while STRIDE is simpler than some other methodologies, effective

implementation still requires a good understanding of security principles and the system being analyzed. Without this expertise, there is a risk that some threats may be overlooked.

In conclusion, STRIDE is a valuable tool for threat modeling that can help organizations identify a wide range of potential security issues. However, to effectively manage security in an IoT context, it may need to be complemented with a risk-based approach and additional IoT-specific considerations.

3. PROPOSED IMPROVEMENTS FOR EXISTING MODELS

Having reviewed the strengths and weaknesses of some existing models for IoT Risk Assessment and Management, we propose the following improvements aimed at addressing the gaps and challenges inherent in the current models:

1. Greater Focus on IoT-Specific Risks: Given the unique nature of IoT ecosystems, improvements propose a more detailed examination of IoT-specific vulnerabilities, such as those related to device heterogeneity, resource constraints, and the impact of real-time operations.
2. Integration of AI and Machine Learning Techniques: As IoT environments are inherently dynamic, traditional static risk assessment approaches may fall short. There is a growing recognition of the potential benefits of integrating AI and machine learning techniques into risk assessment models. With the vast amount of data generated by IoT devices, employing advanced analytics, machine learning, and AI can help in automated risk detection, assessment, and management. This could significantly improve the speed and scalability of risk management models in large-scale IoT systems.
3. Enhanced Quantification of Risks: Some improvements suggest more sophisticated methods of quantifying risks, including the integration of economic models, to better align risk management with business decision-making processes.
4. Handling Scalability: IoT environments are typically characterized by a large number of devices, making scalability an essential factor. Given the scope and scale of IoT, models need to be scalable to effectively manage risk in large IoT ecosystems. This could involve modular or hierarchical approaches that can handle complexity without becoming unmanageable. Improved models should thus be able to efficiently manage risks in large-scale IoT networks.
5. Security by Design: It is often proposed that security should be integrated into the design of IoT systems rather than added as an afterthought. This "security by design" principle can be more effectively incorporated into risk management models.
6. Consideration of Human Factors: As IoT systems often interact directly with users in a variety of contexts, improvements propose a more explicit consideration of human factors in risk assessment and management models.
7. Dynamic and Adaptive Models: Given the rapidly evolving nature of IoT ecosystems and associated threats, proposed improvements emphasize the need for risk assessment models to be dynamic and adaptive, capable of evolving with the changing threat landscape.
8. Holistic Approach: Improvements propose a more holistic view that looks beyond the technology itself to consider organizational and societal implications, including issues related to privacy, ethics, and regulatory compliance.

The proposed improvements aim to better tailor risk assessment and management models to the unique characteristics and challenges of IoT environments, to integrate advanced computational techniques, and to adopt a more holistic and dynamic view of risk management. As IoT continues to evolve and expand, these improvements will need to be continually reassessed and refined.

1. Introduction of a New Model: The IoT Risk Assessment and Management Model (IoT-RAM)

Having evaluated current and identified possible areas of improvement, we propose a new model to address the identified weaknesses and challenges for the current models, the IoT Risk Assessment and Management (IoT-RAM) model. The IoT-RAM model is a novel approach aimed at addressing the unique challenges posed by Internet of Things (IoT) environments in terms of security risk assessment and management. Designed to enhance existing methodologies, this model incorporates the dynamism and complexity of IoT ecosystems and offers a comprehensive, scalable, and practical framework.

The proposed IoT-RAM comprises of the following steps:

1. IoT Asset Identification: This would include IoT devices, data, and systems that could be affected by cybersecurity risks.
2. Data Collection: A stage to represent the process of gathering data from identified IoT devices, user interactions, network traffic, etc.
3. AI-Enhanced Risk Identification: Connected to the second stage. Here, AI algorithms help automatically identify potential threats and vulnerabilities.
4. AI-Powered Risk Analysis: Connected to the third stage. In this stage, AI incorporates probabilistic models and methodologies and assists in estimating the likelihood and potential impact of identified risks.
5. AI-Enabled Risk Evaluation: A stage where AI could assist with evaluating the risks against established criteria to rank and prioritize them based on their potential impact.
6. AI-Driven Risk Mitigation: This stage involves devising strategies and actions to manage and reduce the identified risks.
7. AI-Driven Proactive Implementation of Controls: This would involve putting the decided strategies into action. AI could aid in devising and implementing mitigation strategies to reduce or eliminate the identified risks.
8. AI-Enabled Continuous Monitoring and Review: An arrow loops back from the "Risk Mitigation" stage to the "Data Collection" stage. This represents the use of AI to continuously monitor the system and update the risk profile.
9. AI-Enabled Report Generation and Communication: Finally, appropriate reports are generated and automatically communicated to users and relevant security experts.

The IoT-RAM model incorporates several features:

- IoT-specific Considerations: IoT-RAM is designed specifically with the IoT environment in mind, considering the diversity and the vast number of connected devices, interoperability issues, and unique data privacy concerns inherent to IoT.

- Dynamic Risk Assessment: Given the rapid evolution of IoT technologies and associated threats, IoT-RAM proposes a dynamic approach to risk assessments. This involves continuous monitoring and regular updating of risk assessments to reflect changes in the IoT environment and threat landscape as new threats emerge and existing ones evolve.
- Holistic Security Measures: The model includes comprehensive security measures that span across all layers of the IoT architecture, from physical devices to network and application layers, ensuring a robust defense against a wide array of potential threats.
- Scalability: Recognizing the broad scale of many IoT deployments, the IoT-RAM model is designed to be scalable. This could involve the use of automated tools or algorithms to perform risk assessments across a large number of devices or system components to support automated risk assessment processes for managing large numbers of devices and systems.
- Quantitative Risk Evaluation: IoT-RAM model promotes a quantitative approach to risk evaluation, thus incorporating probabilistic models and methodologies for estimating the likelihood and potential impact of various threats. This can help organizations better understand the potential impact of various threats and make more informed decisions about where to allocate resources.
- User-friendly and Accessible: The model aims to be accessible and straightforward, helping not only security experts but also those without extensive technical knowledge to understand and manage IoT risks effectively.
- IoT-Specific Risk Factors: Unlike traditional risk assessment models, the IoT-RAM model incorporates risk factors that are uniquely related to IoT. This includes considerations around the vast and diverse nature of IoT devices, interoperability issues, data privacy concerns, and the rapid evolution of IoT technologies and associated threats.
- Comprehensive Security Measures: The IoT-RAM model promotes the implementation of security measures that span across all layers of the IoT architecture. This involves taking a holistic approach to security that covers the physical devices, the network, and the application layers.
- Simplification for Non-Experts: The IoT-RAM model aims to make risk assessment and management more accessible to non-experts. This may involve the development of user-friendly tools and guides or the use of simplified language and concepts.

The IoT-RAM model provides a targeted approach to risk assessment and management in IoT environments. Its core tenets offer a way forward in tackling the unique and complex security challenges presented by IoT, delivering a proactive and comprehensive solution for organizations navigating the IoT landscape.

2. Comparative Analysis of Existing Models with the IoT-RAM Model

Existing risk assessment and management models, like NIST SP 800-30, ISO/IEC 27005, FAIR, STRIDE, and OCTAVE, provide a robust foundation for understanding and addressing cybersecurity risks. However, they were not designed specifically for IoT and, therefore, may not fully address the unique characteristics and challenges posed by IoT environments.

Here is a comparison of the existing models with the IoT-RAM:

Scope: Existing models, while comprehensive, are typically designed with a broader scope in mind, encompassing information security in a more general context. The IoT-RAM model, however, is tailored specifically to the complexities and intricacies of IoT.

IoT-Specific Considerations: Existing models may not account for specific IoT-related issues, such as the sheer number and heterogeneity of IoT devices, interoperability concerns, real-time constraints, and issues related to the large scale of IoT deployments. The IoT-RAM model aims to integrate these considerations into the risk assessment and management process.

Dynamic Risk Assessment: Existing models often take a static view of risk, conducting assessments at specific points in time. The IoT-RAM model, recognizing the fast-paced and dynamic nature of IoT, proposes continuous monitoring and updating of risk assessments.

Scalability: With the potential for millions or even billions of IoT devices in a single system, the scalability of risk assessment processes becomes crucial. While existing models can struggle to address this issue, the IoT-RAM model emphasizes scalability.

Quantitative Risk Evaluation: Models like FAIR focus on quantitative risk evaluation, but not all existing models do. The IoT-RAM model encourages a quantitative approach, helping organizations to better understand the potential impact and probability of various threats.

Simplification for Non-Experts: While existing models often require a deep understanding of cybersecurity concepts, the IoT-RAM model aims to make the risk assessment process more accessible to non-experts.

The IoT-RAM model seeks to build on the strengths of existing models while addressing their limitations in the context of IoT. It provides a more IoT-centric, dynamic, scalable, and user-friendly approach to risk assessment and management.

4. CONCLUSION AND FUTURE WORK

This paper introduces a guiding model for IoT security risk management strategies. It is designed to assist professionals from organizations that are utilizing IoT technologies, helping them create or redesign their IoT security risk management strategies to secure their adoption of the Internet of Things (IoT). Additionally, it will serve as a valuable resource for academic researchers who are investigating IoT security risk management strategies in their scholarly pursuits. This work outlined the rapidly evolving landscape of Internet of Things (IoT) technology by reviewing existing models and evaluated their ability to address the unique challenges posed by IoT, identified weaknesses, and proposed innovative improvements to address identified gaps. Subsequently, the work proposed a new model, the IoT Risk Assessment and Management (IoT-RAM) Model, aimed at addressing the unique challenges posed by Internet of Things (IoT) environments in terms of cybersecurity risk assessment and management.

REFERENCES

Al Fikri, M., Putra, F. A., Suryanto,Y., and Ramli, K., (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency, Procedia Computer Science, Vol. 161, 2019, pp. 1206-1215, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2019.11.234.

Alshboul, Y. and Streff, K. (2015) Analyzing Information Security Model for Small-Medium Sized Businesses,

Twenty-first Americas Conference on Information Systems, Puerto Rico 2015 (pp. 1-9)

Balbix, (2022) FAIR Model for Risk Quantification – Pros and Cons, https://www.balbix.com/insights/fair-model-for-risk-quantification-pros-and-cons/ Accessed 26 May 2022.

Berman, Daniel & Buczak, Anna & Chavis, Jeffrey & Corbett, Cherita. (2019). A Survey of Deep Learning Methods for Cyber Security. Information. 10. 122.10.3390/info10040122.

Cyvatar (2022) What is NIST SP 800-30? https://cyvatar.ai/nist-csf-sp-800-30/ Accessed 26 May 2022.

Cyrus, C. (2021) IoT Cyberattacks Escalate in 2021, According to Kaspersky, 17th September 2021, Available online:https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/. Accessed 26 May 2022.

Das, S., Saha, S., Priyoti, A. T., Roy, E. K., Sheldon, F. T., Haque, A., & Shiva, S. (2021). Network intrusion detection and comparative analysis using ensemble machine learning and feature selection. IEEE Transactions on Network and Service Management.

Defense Lead (2021) STRIDE Methodology in Threat Modeling Process, https://defenselead.com/stride-methodology-in-threat-modeling-process/ Accessed 26 May 2022.

Dhillon, G (2016) What to do before and after a Cybersecurity Breach? Virginia Commonwealth University, Richmond, Virginia, USA

Fair Institute (2022) What is FAIR? https://www.fairinstitute.org/what-is-fair

Fair Institute (2022) FAIR Risk Management, https://www.fairinstitute.org/fair-risk-management

Hashim, N. A., Abidin, Z. Z., Puvanasvaran, A. P., Zakaria, N. A., & Ahmad, R. (2018). Risk assessment method for insider threats in cyber security: A review. International Journal of Advanced Computer Science and Applications, 9(11).

Kaur, G., Lashkari, A.H. (2021). Information Technology Risk Management. In: Daimi, K., Peoples, C. (eds) Advances in Cybersecurity Management. Springer, Cham. https://doi.org/10.1007/978-3-030-71381-2_13

Kim, K. H., Kim, K., & Kim, H. K. (2022). STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI Journal*.

Michael Chui, Mark Collins, Mark Patel (2021) The Internet of Things: Catching up to an accelerating opportunity, McKinsey & Company.

Meneghello, Francesca & Calore, Matteo & Zucchetto, Daniel & Polese, Michele & Zanella, Andrea. (2019). IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2019.2935189.

National Institute of Standards and Technology (2021) Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. Available online: https://doi.org/10.6028/NIST.CSWP.04162018. Accessed 26 May 2022..

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). Available online: https://doi.org/10.6028/NIST.CSWP.04162018. Accessed 26 May 2022.

National Institute of Standards and Technology, (2012) NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

Osanaiye O. A., Ogundile O. O. & Aina F. (2022). Evaluating DoS jamming attack on reactive routing protocol in wireless sensor networks, *African Journal of Science, Technology, Innovation and Development,* 14 (5), 1369-1376

Patiño, S., Solís, E. F., Yoo, S. G., & Arroyo, R. (2018, April). ICT risk management methodology proposal for governmental entities based on ISO/IEC 27005. In *2018 International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 75-82). IEEE.

Petar Radanliev, David Charles De Roure, Razvan Nicolescu, Michael Huth, Rafael Mantilla Montalvo, Stacy Cannady, Peter Burnap, Future developments in cyber risk assessment for the internet of things, Computers in Industry, Volume 102, 2018, Pages 14-22, ISSN 0166-3615, https://doi.org/10.1016/j.compind.2018.08.002. Accessed 26 May 2022.

Radanliev, P.; De Roure, D.; R.C. Nurse, J.; Burnap, P.; Anthi, E.; Ani, U.; Maddox, L.; Santos, O.; Mantilla Montalvo, R. Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment. Preprints 2019, 2019030080 doi:10.20944/preprints201903.0080.v1).

Radanliev, Petar, David, De Roure, Jason R.C. Nurse, Rafael Mantilla Montalvo, Stacy Cannady, Omar Santos, La'Treall Madox, Peter Burnap, and Carsten Maple (2020). "Future Developments in Standardisation of Cyber Risk in the Internet of Things (IoT)." SN Applied Sciences, no. 2: 169 1–16. https://doi.org/10.1007/s42452-019-1931-0. Accessed 16 May 2022

The Open Group (January 2009) Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081, https://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf Accessed 26 May 2022.

Patiño, S., Solís, E. F., Yoo, S. G., & Arroyo, R. (2018, April). ICT risk management methodology proposal for governmental entities based on ISO/IEC 27005. In 2018 International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 75-82). IEEE.

Popescu, T.M, Popescu, A.M. and Prostean, G. (2021). Leaders' Perspectives on IoT Security Risk Management Strategies in Surveyed Organizations Relative to IoTSRM2. Applied Sciences. 11. 9206.10.3390/app11199206.

Popescu, T.M, Popescu, A.M. and Prostean, G. (2021) IoT Security RiskManagement Strategy Reference Model (IoTSRM2), Future Internet, 13, 148. https://doi.org/10.3390/fi13060148 Accessed 26 May 2022.

Radanliev, P., De Roure, D., Nurse, J. R., Nicolescu, R., Huth, M., Cannady, S., & Montalvo, R. M. (2018, March). Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1-6). IET.

Sunflower-cissp (2019) OCTAVE, https://www.sunflower-issp.com/glossary/cissp/5506/octave Accessed 26 May 2022.

Viswanathan, G., & Jayagopal, P. (2021). A Threat Categorization of Risk-Based approach for analyzing Security Threats early phase in SDLC. Arabian Journal for Science and Engineering, 1-13.

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. International Journal of Information Security, 17, 681-699. https://doi.org/10.1007/s10207-017-0382-0 Accessed 26 May 2022.

NIST, 2012 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf Accessed 26 May

2022.

Whitman, Michael E.; Mattord, Herbert J. (18 October 2013). Management of Information Security. Cengage Learning. ISBN 978-1-305-15603-6.