Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

A SECURITY ASSURANCE CASE FOR IoT SYSTEMS USING GOAL STRUCTURE NOTATION

Aftab Alam Janisar[1*], Khairul Shafee Kalid[2], Aliza Sarlan[3], Abdul Rehman Gilal[4], M. Aqeel Iqbal[5], Muhammad Aamir Khan[6]

[1] Department of Computer and Information Science Universiti Teknologi Petronas, 32610 Seri Iskandar Perak Malaysia.
Emails: aftab_22001362@utp.edu.my
[2] Department of Computer and Information Science Universiti Teknologi Petronas, 32610 Seri Iskandar Perak Malaysia.
Emails: khairulshafee_kalid@utp.edu.my
[3] Department of Computer and Information Science Universiti Teknologi Petronas, 32610 Seri Iskandar Perak Malaysia.
Emails: aliza_sarlan@utp.edu.my
[4] Florida International University, 11200 SW 8th St, Miami, FL 33199, USA
Emails: arehman@fiu.edu
[5] Department of Software Engineering Faculty of Engineering & Information Technology Foundation University Islamabad, Pakistan.
Emails: maqeeliqbal@fui.edu.pk
[6] School of Computing Sciences, College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, 40450, Shah Alam, Selangor, Malaysia.
Emails: amirkhan@uitm.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 29.01.2025
Revised date: 12.02.2025
Accepted date: 17.03.2025
Published date: 30.03.2025

To cite this document:

Janisar, A. A., Khalid, K. S., Sarlan, A., Gilal, A. R., Iqbal, M. A., & Khan, M. A. (2025 A Security Assurance Case For IoT Systems Using Goal Structure Notation. *Journal of Information System and Technology Management, 10* (38), 381-395.

Abstract:

IoT-focused cyberattacks had the largest attack surface, despite having a vast environment. Key security requirements (SR) for IoT include data confidentiality, data integrity, authentication, access control, privacy, etc. On the Internet of Things, confidentiality is a crucial security service and the most frequently targeted. Inadequate emphasis on assessment of IoT (SR) leads to attacks and threats. However, the absence of security requirement assessment in IoT systems architecture jeopardizes security, exposing the system to vulnerabilities, risking organizational assets and reputation, while also escalating the cost and time required to address security issues. An assurance case is developed for identification of security requirements assessment based on compliance standards. To communicate, align IoT security measures, and to identify, analyze, and address potential assets, security threats, and attacks systematically. In this research, a novel and illustrative example of assurance case is provided for the confidentiality security requirement of IoT system, to shed light on possible attacks and threats relevant to IoT assets. This process will help leverage a

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

DOI: 10.35631/JISTM.1038026

practical and clear basis for justifiable development of assurance case for IoT security requirement earlier and integration with RE activities. This structured approach will be vital across methodologies like Agile, Waterfall, and SSDL, ensuring compliance with security standards and offering a comprehensive solution to key challenges in IoT security.

Keywords:

Security Requirement Engineering (SRE), Requirement Engineering (RE), Software Security, Security Requirements Assurance, Assurance Case

Introduction

Organizations and businesses are becoming more aware of information and related technologies, particularly in terms of innovation and competitive advantage generation. In the contemporary information age, both business information and technology service solutions are vulnerable to a diverse array of security risks and threats, such as the leakage of sensitive data from users, which significantly hurt automated systems, cyber-physical systems and business continuity.

IoT security is one of the biggest problems in cyber security because the proliferation of IoT devices is expanding rapidly. Given that IoT devices are connected online, serious threats and attacks can happen in the IoT environment. IoT has become instrumental across multiple sectors including smart grids, healthcare, homes, transportation, environmental monitoring, and urban infrastructure (Alshdadi et al., 2024). However, despite its widespread adoption, IoT-focused cyberattacks are characterized by the largest attack surface. IoT cyberattack would be catastrophic for business continuity (Kimani et al., 2019).

To address the security issues that threaten the IoT environment, additional security measures are required to protect IoT-based applications from threats and other vulnerabilities (Abdullahi et al., 2022). As a result, security has emerged as a major concern for both researchers and practitioners (Humayun et al., 2020). Computer assets that belong to a company or that connect to another company's network must be protected so that their integrity, confidentiality, and availability (CIA) are not compromised in any way (Kaur & Ramkumar, 2022). Key security requirements for IoT, including data confidentiality, integrity, authentication, access control, and privacy, etc. Consequently, the identification of these security measures presents a formidable challenge, given the diverse array of threats and attacks targeting IoT software systems. (Shukla et al., 2022) (Lins & Vieira, 2020). Threats and attacks can be directed from any stage of SDLC (Wheeler et al., 2018). Indeed, requirement engineering stands as the initial and pivotal stage. However, it's imperative to conduct an assessment and evaluation of the identified security requirements (Katt & Prasher, 2019).

Awareness regarding software security vulnerabilities has expanded beyond critical software systems to encompass non-critical software systems, which has a significant impact on the general population. Therefore, integration and assessment security requirements from the beginning not only guarantees secure software but also saves time and reduces the amount of rework required by the software development team (Hibshi et al., 2021). So, discussing the security challenges in IoT along with potential solutions can help developers and businesses find the right strategies to deal with specific threats, ensuring they deliver top-notch IoT services (HaddadPajouh et al., 2021). The IoT security requirements encompass data

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

confidentiality, integrity, authentication, access control, privacy, and more. Confidentiality involves preventing unauthorized access to private data, ensuring that only authorized entities can view, modify, or remove personal information. In the context of IoT, confidentiality is a crucial security service but also one of the most targeted (Azrour et al., 2021).

However, Security requirement identification is a challenging task due to the sheer number of threats and attacks to an IoT system. There is a lack of a structural relationship between the security requirements assurance, and its assessment (Shukla et al., 2021). Previous studies offer methods and approaches for evaluating security requirements, but none of them specifically highlight a crucial factor in security assessment in IoT.

Security assurance ensures that systems meet security requirements and withstand potential threats. With the growing number of software security risks and increased awareness, software security assurance is now a necessity, not a choice (Khan & Khan, 2018; Zhou et al., 2021). A security assurance case (SAC) or security case is a structured collection of arguments used to justify the security of a software system based on available evidence. SACs offer a new method for ensuring the secure development of critical systems, particularly in business sectors. (Kabir, 2021) (Mohamad et al., 2021). The contribution of this study is given below, "This study unveils novel insights into the integration of security requirements early in the Development Life Cycle IoT systems, by leveraging the security compliance standard, it demonstrates a structured and methodical assurance process for security requirements, emphasizing the efficacy of Security Requirement assurance and highlighting a crucial gap in understanding Security Requirement in IoT system." Specific threats and attack vectors targeting critical IoT system assets are identified, enabling a deeper understanding of risk areas and the corresponding security measures needed.

Top Level assurance case is decomposed further into specific security requirements “Confidentiality” with detailed arguments, strategies, assumptions, and justifications.

The rest of this paper follows this structure: Background is covered in Section 2. Section 3 delves into related work. Assurance Case Development Process is detailed in Section 4, while Section 5 concludes the paper.

Background

Requirements serve as crucial foundations and integral phases of software development (Mishra & Mustafa, 2020). However, security concerns are often addressed as an afterthought by software engineers, rather than as a continuous process throughout development. It's essential to incorporate security measures at every stage of the software development lifecycle (Humayun et al., 2023; Nazir & Nazir, 2018). Security is commonly deemed paramount in software, ensuring the protection of information and data, typically characterized by the CIA trio: Confidentiality, Integrity, and Availability (Flores & Meira, 2021). Consequently, security holds the highest priority in software development in the present era.

Security Requirements

Security requirements constrain system functions to achieve specific security objectives (Anwar Mohammad et al., 2019). Defined security requirements are occasionally mistaken for security-specific architectural limitations, hindering the security team's ability to employ optimal security techniques to meet genuine security requirements (Niazi et al., 2020).

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

Practitioners and researchers advise including security-related aspects during the requirement phase to prevent rework and mitigate the spread of problems in later stages (Qadir & Ahmad, 2022) Security requirements are categorized into various types of properties, each targeting specific aspects of security threats and assets. Key security Requirements are confidentiality, Integrity, Availability, Authentication, Access Control and privacy.

Security Assurance Case

Assurance cases, following the GSN standard, are structured, evidence-backed arguments ensuring a system's intended operation. Security Assurance Cases (SACs) focus on security claims with evidence. These cases demonstrate system compliance with specified requirements, helping identify and manage security risks (Zhou et al., 2021). They provide auditable artifacts supporting claims through systematic reasoning, evidence, and clear assumptions, as per ISO/IEC/IEEE standards (Kläs et al., 2021).

Related Work

This study takes a different approach from earlier research, which mostly looked into safety assurance cases, by concentrating on security assurance cases instead. Table 1 outlines the relevant literature about both security and safety assurance cases (Janisar et al., 2023).

Table 1: Literature Relevant to Assurance Cases

Study	Descriptions
(Chelouati et al., 2023)	The study explores GSN for autonomous train safety cases, highlighting its role in improving traceability, compliance, and clarity in safety argumentation.
(Kläs et al., 2021)	This paper discusses assurance cases for AI, emphasizing the importance of risk minimization and structured safety claims.
(Lin et al., 2020)	This study concentrates on automating the GSN model to assess the confidence level of assurance cases in safety-critical systems.
(Zhou et al., 2021)	Focuses on automating GSN to evaluate assurance case confidence in safety-critical systems.
(Almendra et al., 2019)	Integrates assurance cases with Agile, proposing a model for incremental development.
(Cârlan & Ratiu, 2020)	Describes FASTEN Safe, automating GSN verification for consistency.
(Wei et al., 2019)	Explores SACM's benefits in adaptive system assurance but notes standardization challenges.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

Figure 1 illustrates three key elements of an Assurance case on the left side: Top-level claims representing achieved objectives, supporting argumentation, and Underlying evidence. On the right side of the figure, Argumentation (reasoning) and assumptions are structured like a tree, connecting lower-level claims to higher claims, with assumptions explicitly stated as needed. Various languages, such as Goals Structuring Notation (GSN) and Claim Argument Evidence Notation, can be employed to model Assurance cases effectively (Janisar et al., 2023; Kläs et al., 2021).

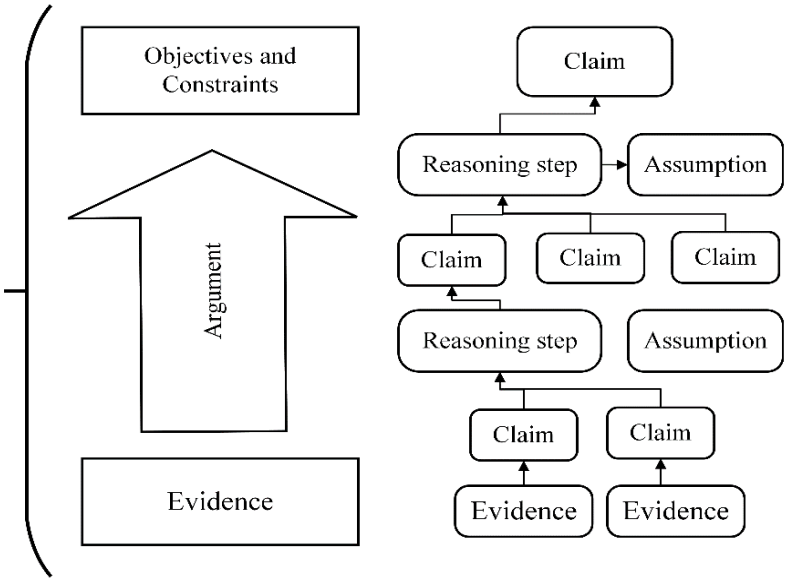

Figure 1: Assurance Case Common Structure

Assurance Case Development Process

The objective of this study is to establish a comprehensive understanding of security assurance case and to develop a structured assurance case. The diagram represents the Goal Structuring Notation (GSN) elements, which are essential components used to construct assurance cases. Here is a brief description of each element:

- Goal: Represents the main objectives or claims being made in the assurance case.
- Strategy: Describes the approach taken to decompose a high-level goal into sub-goals or claims.
- Assumption: Indicates conditions or premises assumed to be true for the argument to hold.
- Context: Provides the background or environmental information relevant to the goal or strategy.
- Justification: Explains why the strategy or argument is valid or reasonable.
- Solution: Provides evidence, such as data or artifacts, that supports the claim or goal.
- Undeveloped Goal: Represents a goal that has not yet been fully developed or supported.
- Undeveloped Solution: Indicates a solution that requires further elaboration or evidence.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

- InContextOf: Links a goal, strategy, or solution to its relevant context.
- SupportedBy: Links a goal to its supporting strategy, evidence, or sub-goals.

Security requirements for software applications can be elucidated using Security Assurance Cases (SAC), presented as structured arguments supported by evidence (Cheng et al., 2018). Assurance approaches assume that different abstraction levels of security claims made on the system correspond to various stages of software development (requirements, design, implementation, and deployment) (Mohamad et al., 2021) (Maksimov et al., 2019). Initially, Assurance Case was predominantly utilized for safety-critical systems and was referred to as a "Safety Case." However, the escalating security concerns prompted the development of a "Security Case" or security-informed Safety Case (Sklyar et al., 2017). A comprehensive set of functional safety requirements for controlling systems can be found in a series of industrial standards, such as IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems." The assurance case is constructed utilizing the Goal Structuring Notation (GSN) figure 2, focusing specifically on addressing the security requirements of IoT systems. This assurance case underwent rigorous review cycles within our group until we were confident that all pertinent arguments had been addressed, mitigating significant risks to the security requirements of IoT systems.

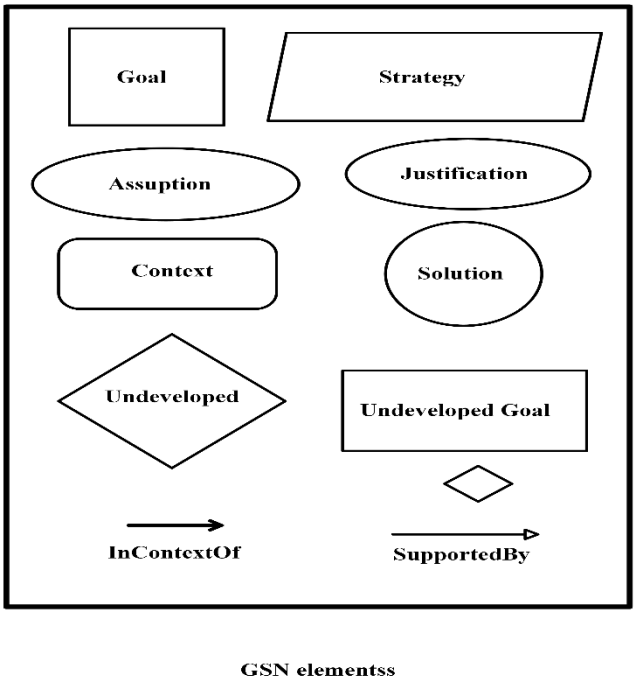

Figure 2: Common Structure of GSN elements

Top Level Assurance Case

Set forth the overarching claims that the system should be adequately safeguarded against moderate threats, as illustrated in the top-level diagram of Figure 3 (Wheeler et al., 2018). To support this claim, decompose the top-level claim into two subordinate claims:

1) Security implemented by the software lifecycle process.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

Security requirements are identified and fulfilled through functional capabilities to counter threats.

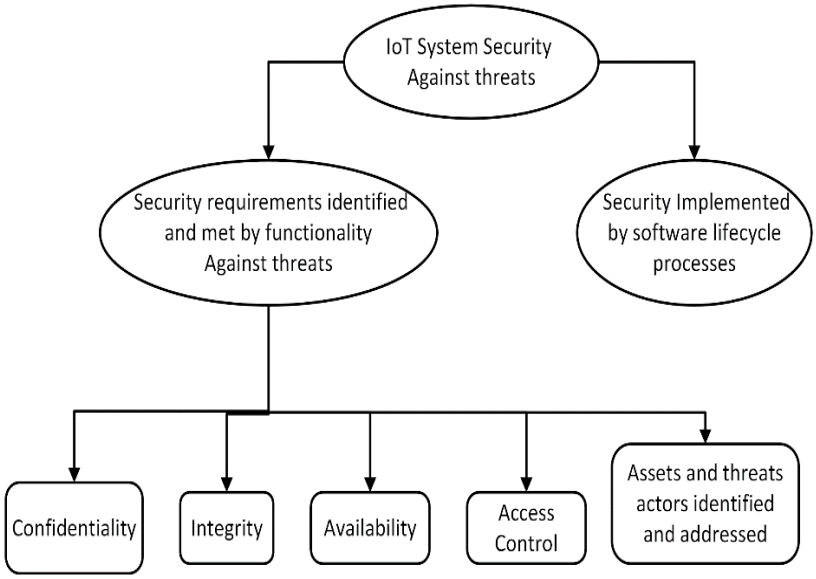

Figure 3: Top Level Assurance Case

Ensuring that security requirements are both identified and fulfilled by system functionality is paramount. Without clear knowledge of these security prerequisites, it becomes impossible to ascertain whether the system adequately addresses them. This requires understanding the system's core security requirements, which include confidentiality, integrity, and availability. These fundamental security requirements must be effectively supported by access control mechanisms, specifically identification, authentication, and authorization. A thorough comprehension of the security requirements also involves identifying and mitigating threats against the system's protected assets and potential threat actors. The detailed security requirements depicted in the top-level diagram are specific to each system in Figure 3. For example, while most systems need to maintain confidentiality of certain information, the specifics can vary, including the type of information to be kept confidential, the threat actors to be guarded against, and how access control is managed to authorize information access.

Assurance case for IoT Security Requirement

In the pursuit of ensuring the security of Internet of Things (IoT) systems and facilitating seamless communication among their interconnected devices, the goal (G1) focuses on ensuring IoT systems' security and enabling secure communication among interconnected devices, emphasizing the critical need for robust protections in IoT environments Figure 4. To achieve this, the approach emphasizes the core elements required to maintain security in any system, strategy (S1) adopts the CIA Confidentiality (G2), Integrity (G3), and Availability (G4). This strategy is supported by the context (C1), which defines "acceptably secure" based on the assumption that addressing CIA adequately fulfils IoT security requirements. However, the term "acceptably secure" lacks measurable benchmarks, making the evaluation subjective. The argument further assumes that pertinent security properties can be extracted from system specifications, which might not always hold in poorly documented systems. While this framework logically organizes security objectives, it narrowly focuses on the CIA triad, excluding other critical aspects such as authentication or non-repudiation. Additionally,

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

reliance on comprehensive documentation introduces potential gaps in identifying security needs.

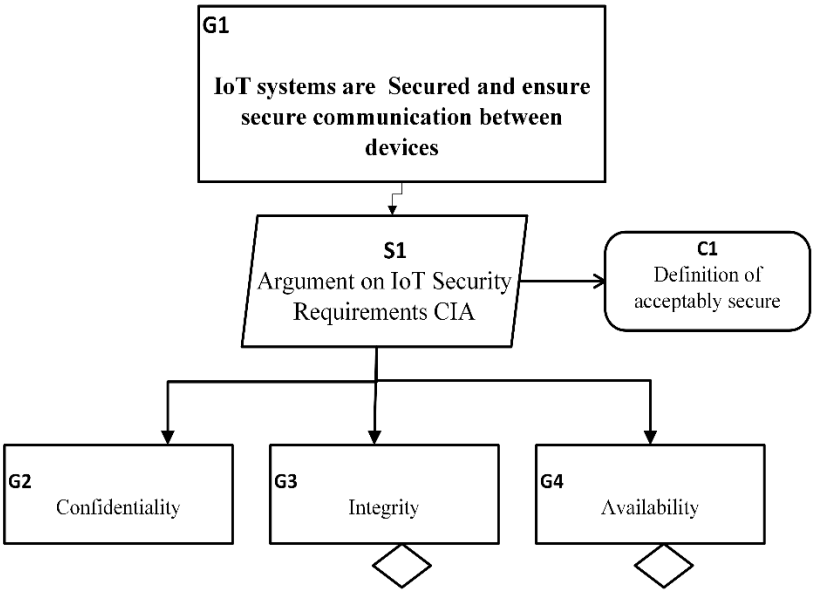

Figure 4: Top level Goal (G1)

The model-driven approach supports Goal (G2) – Confidentiality – through Strategy (S2), as shown in
Figure **5**, which outlines the necessary steps to secure IoT system components. Assumptions (A1) state that all IoT assets are protected by strong security measures, with justification (J1) relying on the correct implementation of security protocols. While this approach provides clarity, there are challenges in practice. The assumption that all assets are secure may not hold in real-world scenarios, as IoT devices often face vulnerabilities due to inconsistent security standards and rapid technological changes. Moreover, depending on the proper implementation of protocols, it assumes that all stakeholders possess the required expertise, which is not always guaranteed. The breakdown of Goal (G2) into specific objectives such as Sensors (G5), Hardware/Devices (G6), Communication Links (G7), Gateway (G8), and User Interface (G9) offers structure but may oversimplify the complexities of ensuring confidentiality across these diverse components. Each of these objectives presents unique challenges, such as potential vulnerabilities in communication links or unauthorized access to user interfaces. While the strategy aims to provide comprehensive protection, it must account for the dynamic nature of IoT systems and address evolving threats to maintain effective confidentiality needs.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

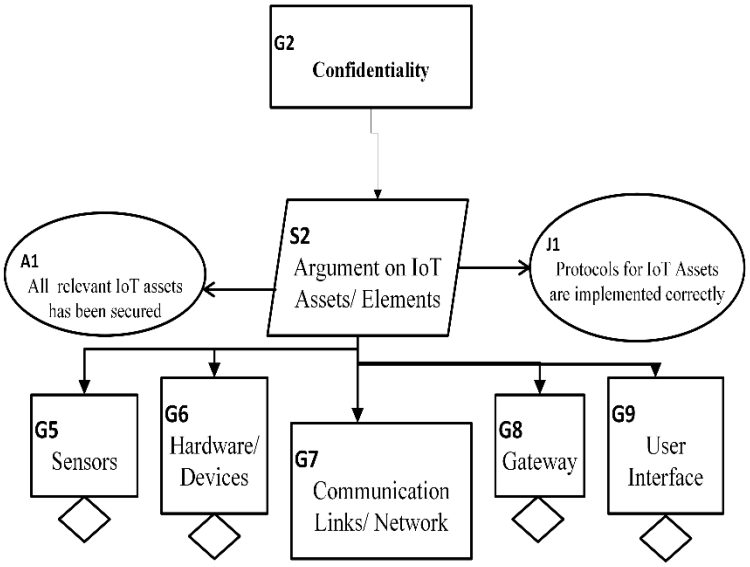

Figure 5: Sub Module/Goal (G2)

Goal (G7) – Communication Links – is supported by Strategy (S3), which emphasizes the importance of identifying and mitigating threats that affect communication links within IoT systems, as depicted in figure 6. Assumptions (A2) are established regarding the comprehensive identification of principal threats to these links. Further dissection of Goal (G7) into sub-goals such as (G10, unauthorized access), (G11, control over device), (G12, Eavesdropping), (G13, Protocol vulnerabilities), and (G14, Physical device threats) underscores the range of potential threats demanding attention. While this process presents a comprehensive approach, it presupposes that all critical threats are thoroughly identified and managed, which may not always hold in the rapidly changing domain of IoT. While certain risks, such as unauthorized access or eavesdropping, are well-documented, new vulnerabilities—like emerging concerns with communication protocols—can arise more swiftly than they can be resolved. Furthermore, the process assumes that all involved stakeholders possess the requisite expertise to accurately evaluate and address these risks, which may not consistently be the case, particularly in systems characterized by disparate levels of security expertise.

Let's explore a comprehensive approach to constructing an IoT Assurance Case tailored to security requirements with the specific eavesdropping threat elaborated in Table 2.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

Threat	*Asset*	*Attack*
Eavesdropping	Communication networks	• Replay attack. • Eavesdropping • Dos/DDoS • Hijacking • Jamming • MIM • Insider attack

Table 2: Identified Threats/Assets and Attacks

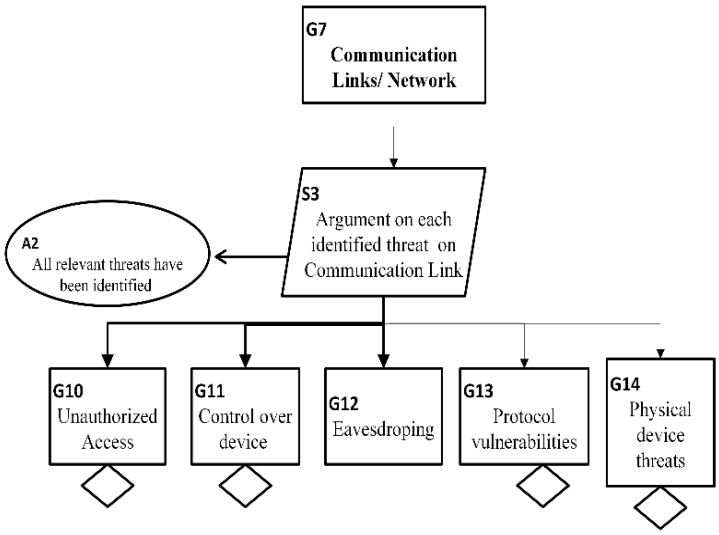

Figure 6: Sub Module/Goal (G7)

Eavesdropping poses a significant threat to IoT communication links due to the widespread accessibility of IoT devices and their limited resources (Al-Garadi et al., 2020) (Alharbi et al., 2022). Within IoT systems, security challenges vary based on network characteristics, including issues such as data volume, scalability, heterogeneity, interoperability, autonomous control, and resistance to attacks (Ogonji et al., 2020). These challenges generate vast amounts of sensitive data, necessitating stringent privacy protection measures (Ogonji et al., 2020). Communication security protocols encompass key elements such as confidentiality, integrity, and usability, all of which are crucial for ensuring the security of IoT communication links (Al-Garadi et al., 2020) .

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

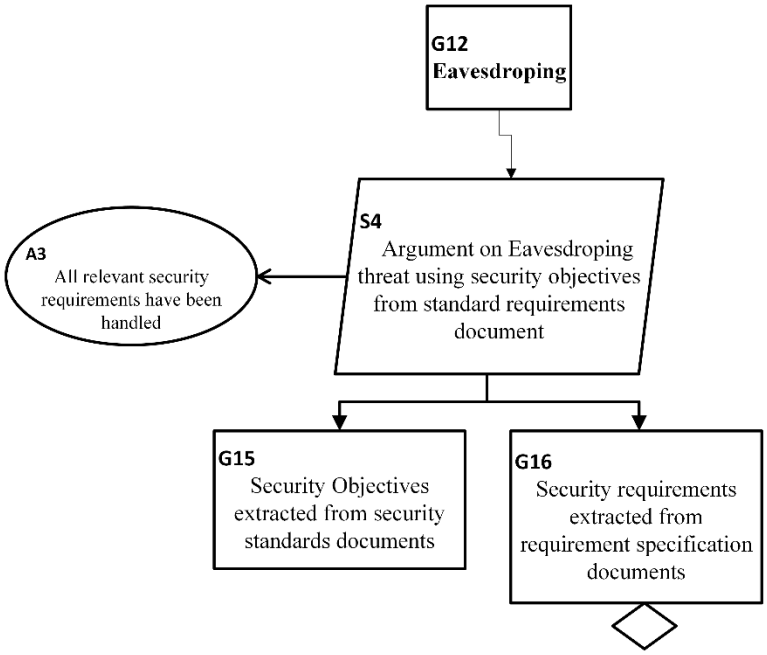

Figure 7: Sub Module/Goal (G12)

In IoT environments, eavesdropping attacks severely compromise data confidentiality, jeopardizing the privacy and integrity of exchanged information (Wu et al., 2023). Unauthorized interception of messages transmitted over open channels can lead to malicious access to users' private data, highlighting the critical need for privacy protection (Wu et al., 2023). Such attacks undermine the confidentiality and integrity of data transmitted by IoT devices, necessitating robust encryption and security measures to mitigate risks (Ogonji et al., 2020) (Ali & Awad, 2018). Eavesdropping remains a critical security issue for IoT communication links, underscoring the imperative need for deploying robust encryption and security protocols to mitigate this risk.

Strategy (S4) provides mitigation approaches for addressing eavesdropping threats on IoT communication links, as shown in Figure 7. These strategies are based on security objectives outlined in relevant security standards. Assumptions (A3) suggest that these threats will be effectively managed through adherence to established security standards. After this, Goal (G12) is further decomposed into sub-goals, including (G15) security objectives established from security standards and (G16) security prerequisites formulated from security requirement specification documents, which define the essential procedures for extracting security requirements from pertinent sources. While the approach appears robust, it relies heavily on the assumption that adherence to these standards is sufficient to mitigate eavesdropping risks, overlooking the potential challenges of implementing these standards across varied IoT environments. Moreover, the procedure for extracting security requirements from documentation is assumed that such documents are up-to-date and faithfully represent the current condition, a condition that is not consistently met in rapidly changing technological environments.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

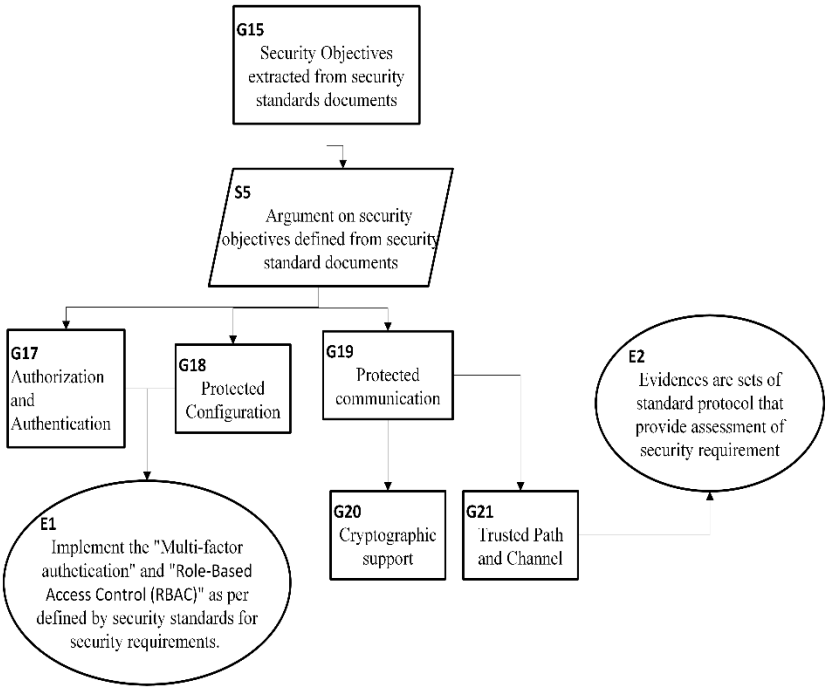

Figure 8: Sub Module/Goal (G15)

Objective (G15) – Security objectives – is supported by Strategy (S5), which outlines the approach for formulating security objectives based on insights derived from security standard documents. Within (G15), the sub-objectives encompass (G17) authorization and authentication, (G18) safeguarded configuration, and (G19) secured communication, with (G19) further segmented into (G20) cryptographic support and (G21) trusted pathways and channels, as illustrated in Figure 8. Evidence (E1) comprises standard protocols that aid in assessing the security prerequisites of IoT communication links concerning threats and related assets. While this strategy offers a systematic approach, it predicates that the security objectives obtained from the standards are exhaustive and relevant across all IoT scenarios.

Conclusion

The rapid growth of IoT has significantly improved human life but also heightened its vulnerability to cyberattacks. This study introduces a security assurance case tailored to the specific assets and threats within IoT security requirements. The proposed assurance case can be integrated into IoT system development, enhancing security and privacy, and reducing the risk of cybercrimes. By adhering to this assurance case, IoT security requirements will be strengthened, contributing to the overall quality of system development. Future work could expand the assurance case methodology to other critical systems, ensuring more robust security practices across various domains.

Acknowledgement

This research was funded by Collaborative Research Fund (CRF) (015ME0-383)".

Conflicts Of Interest

“The authors declare that they have no conflicts of interest to report regarding the present study”.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026

References

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics*, *11*(2). https://doi.org/10.3390/electronics11020198

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646-1685.

Alharbi, S., Attiah, A., & Alghazzawi, D. (2022). Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends. *Sustainability*, *14*(23), 16002.

Ali, B., & Awad, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors (Basel)*, *18*(3). https://doi.org/10.3390/s18030817
10.3390/s18030817.

Almendra, C. C., Barros, F., & Silva, C. (2019). Using Assurance Cases in Requirements Engineering for Safety-Critical Systems. Anais Estendidos do X Congresso Brasileiro de Software: Teoria e Prática,

Alshdadi, A., Kamel, S., Alsolami, E., Lytras, M. D., & Boubaker, S. (2024). An IoT Smart System for Cold Supply Chain Storage and Transportation Management. *Engineering, Technology & Applied Science Research*, *14*(2), 13167-13172.

Anwar Mohammad, M. N., Nazir, M., & Mustafa, K. (2019). A Systematic Review and Analytical Evaluation of Security Requirements Engineering Approaches. *Arabian Journal for Science and Engineering*, *44*(11), 8963-8987. https://doi.org/10.1007/s13369-019-04067-3

Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of things security: challenges and key issues. *Security and Communication Networks*, *2021*, 1-11.

Cârlan, C., & Ratiu, D. (2020). FASTEN. Safe: A model-driven engineering tool to experiment with checkable assurance cases. Computer Safety, Reliability, and Security: 39th International Conference, SAFECOMP 2020, Lisbon, Portugal, September 16–18, 2020, Proceedings 39,

Chelouati, M., Boussif, A., Beugin, J., & El Koursi, E.-M. (2023). Graphical safety assurance case using Goal Structuring Notation (GSN)—challenges, opportunities and a framework for autonomous trains. *Reliability Engineering & System Safety*, *230*, 108933.

Cheng, J., Goodrum, M., Metoyer, R., & Cleland-Huang, J. (2018). *How do practitioners perceive assurance cases in safety-critical software systems?* Proceedings of the 11th International Workshop on Cooperative and Human Aspects of Software Engineering,

Flores, F. F. S., & Meira, S. R. d. L. (2021). *(UN)Ethical Software Engineering : A critical review about Software Engineering in face of Security Requirements in the IoT/ IoE Society* 2021 IEEE International Systems Conference (SysCon),

HaddadPajouh, H., Dehghantanha, A., M. Parizi, R., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*. https://doi.org/10.1016/j.iot.2019.100129

Hibshi, H., Jones, S., & Breaux, T. (2021). A Systemic Approach for Natural Language Scenario Elicitation of Security Requirements. *IEEE Transactions on Dependable and Secure Computing*, 1-1. https://doi.org/10.1109/tdsc.2021.3103109

Humayun, M., Niazi, M., Assiri, M., & Haoues, M. (2023). Secure Global Software Development: A Practitioners' Perspective. *Applied Sciences*, *13*(4). https://doi.org/10.3390/app13042465

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026
Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, 3171-3189.

Janisar, A. A., bin Kalid, K. S., Sarlan, A. B., & Gilal, A. R. (2023). Security Requirements Assurance: An Assurance Case Perspective. 2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS),

Kabir, S. (2021). Internet of Things and Safety Assurance of Cooperative Cyber-Physical Systems: Opportunities and Challenges. *IEEE Internet of Things Magazine*, *4*(2), 74-78. https://doi.org/10.1109/iotm.0001.2000062

Katt, B., & Prasher, N. (2019). Quantitative security assurance. In *Exploring security in software architecture and design* (pp. 15-46). IGI Global.

Kaur, J., & Ramkumar, K. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.

Khan, R. A., & Khan, S. U. (2018). A preliminary structure of software security assurance model. Proceedings of the 13th International Conference on Global Software Engineering,

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36-49. https://doi.org/10.1016/j.ijcip.2019.01.001

Kläs, M., Adler, R., Jöckel, L., Groß, J., & Reich, J. (2021). Using Complementary Risk Acceptance Criteria to Structure Assurance Cases for Safety-Critical AI Components. AISafety@ IJCAI,

Lin, C.-L., Shen, W., & Cheng, B. (2020). Measuring Confidence of Assurance Cases in Safety-Critical Domains.

Lins, F. A. A., & Vieira, M. (2020). Security requirements and solutions for iot gateways: A comprehensive study. *IEEE Internet of Things Journal*, *8*(11), 8667-8679.

Maksimov, M., Kokaly, S., & Chechik, M. (2019). A survey of tool-supported assurance case assessment techniques. *ACM Computing Surveys (CSUR)*, *52*(5), 1-34.

Mishra, A. D., & Mustafa, K. (2020). Security requirements specification: a formal method perspective. 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom),

Mohamad, M., Steghöfer, J.-P., & Scandariato, R. (2021). Security assurance cases—state of the art of an emerging approach. *Empirical Software Engineering*, *26*(4). https://doi.org/10.1007/s10664-021-09971-7

Nazir, N., & Nazir, M. K. (2018). A review of security issues in SDLC. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, *46*(1), 247-259.

Niazi, M., Saeed, A. M., Alshayeb, M., Mahmood, S., & Zafar, S. (2020). A maturity model for secure requirements engineering. *Computers & Security*, *95*. https://doi.org/10.1016/j.cose.2020.101852

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review*, *38*, 100312.

Qadir, N., & Ahmad, R. (2022). SecRS template to aid novice developers in security requirements identification and documentation. *International Journal of Software Engineering and Computer Systems*, *8*(1), 45-52.

Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2021). System security assurance: a systematic literature review. *arXiv preprint arXiv:2110.01904*.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 38 (March 2025) PP. 381-395
DOI: 10.35631/JISTM.1038026
Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. *Computer Science Review*, *45*. https://doi.org/10.1016/j.cosrev.2022.100496

Sklyar, V., Kharchenko, V., & Bardis, N. G. (2017). Assurance case for green IT applications: proof of compliance with power consumption claims. 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI),

Wei, R., Kelly, T. P., Dai, X., Zhao, S., & Hawkins, R. (2019). Model based system assurance using the structured assurance case metamodel. *Journal of Systems and Software*, *154*, 211-233. https://doi.org/10.1016/j.jss.2019.05.013

Wheeler, D. A., Fong, E., & Alexandria, I. f. D. A. (2018). *A Sample Security Assurance Case Pattern*.

Wu, T.-Y., Meng, Q., Chen, Y.-C., Kumari, S., & Chen, C.-M. (2023). Toward a secure smart-home IoT access control scheme based on home registration approach. *Mathematics*, *11*(9), 2123.

Zhou, Z., Matsubara, Y., & Takada, H. (2021). *Quantitative Security Assurance Case for In-vehicle Embedded Systems* 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech),