UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Natalja Kjaernested

IoT security: Graph-based vulnerability and risk assessment models

Master's Thesis (30 ECTS)

Supervisor:
Sedat Akleylek, PhD

Tartu 2025

IoT security: Graph-based vulnerability and risk assessment models

Abstract:

The swift growth of the Internet of Things (IoT) presents major security challenges, as connected devices often lack robust protections against cyber threats. This thesis explores security vulnerabilities in IoT ecosystems and methods for their identification, prioritization, and mitigation. Nessus was used to identify vulnerabilities in IoT environments, while Power BI helped to prioritize the most critical risks by assessing their potential impact. Threat modeling approaches were also analyzed using a case study on CVE-2017-0144, illustrating how risks could be spread to adjacent systems from a single breached server. Neo4j was leveraged to visualize and analyze these attack pathways, enhancing situational awareness.

Given that much of the IoT supply chain is outsourced, third-party risk management strategies were also investigated emphasizing the importance of security assessments of IoT vendors.

Neo4j was leveraged to process Third-Party Risk Management (TPRM) questionnaires, enabling the creation of an overall risk score of IoT suppliers security posture. TPRM questionnaries are a part of threat modelling as they assess security risks, vulnerabilities as well as compliance gaps that contribute to threat identification and mitigation.

Questionnaires used in this research as an example were Due Dilligence, Self-Assessment and Deep Dives. This method implies the respondent – IoT suppliers fills out a predefined questionnaire, covering security controls, compliance, and best practices. Deep Dive Questionnaires from the on-site security assessments imply in-person evaluations, including facility inspections, interviews, and system reviews. Third party services such as BitSight or SecurityScoreBoard help to analyze digital footprints of IoT vendors to provide their security ratings based on the external scan results.

Keywords: Internet of Things (IoT), Threat Modeling, System Vulnerabilities, Risk Management
CERCS: P170 Computer science, numerical analysis, systems, control

IoT turvalisus: graafikupõhised haavatavuse ja riskide hindamise mudelid

Lühikokkuvõte:

Asjade Interneti (IoT) kiire laienemine toob kaasa olulisi turvaprobleeme, kuna ühendatud seadmetel puudub sageli tugev kaitse küberohtude eest. See lõputöö uurib turvaauke IoT ökosüsteemides ning meetodeid nende tuvastamiseks, tähtsuse järjekorda seadmiseks ja leevendamiseks. Nessust kasutati asjade Interneti-keskkondade üksikute haavatavuste avastamiseks, samas kui Power BI-d kasutati kõige kriitilisemate riskide prioriseerimiseks nende võimaliku mõju põhjal.

Lisaks uurisime ohtude modelleerimise lähenemisviise CVE-2017-0144 hõlmava kasutusjuhtumi kaudu, näidates, kuidas üks ohustatud server võib levitada riske lähedalasuvatesse süsteemidesse. Neo4j-d kasutati nende rünnakute visualiseerimiseks ja analüüsimiseks, suurendades olukorrateadlikkust.

Arvestades, et suur osa asjade Interneti tarneahelast on sisseostetud, uurisime ka kolmandate osapoolte riskijuhtimise strateegiaid, rõhutades asjade Interneti tarnijate turbehinnangute olulisust, analüüsisime erinevaid turvaküsimustikke ja töötlesime neid Neo4j abil, et tuvastada müüjad, kellel on kõige suurem kokkupuude haavatavuste ja ohtudega.

Neo4j kasutati kolmanda osapoole riskijuhtimise (TPRM) küsimustike töötlemiseks, mis võimaldas luua asjade Interneti-tarnijate turvapositsiooni üldise riskiskoori. TPRM-i küsimustikud on osa ohtude modelleerimisest, kuna need hindavad nii turvariske, haavatavusi kui ka vastavuslünki, mis aitavad kaasa ohtude tuvastamisele ja leevendamisele.

Selles uuringus kasutati näiteks küsimustikke Due Dilligence, Self-Assessment ja Deep Dives. See meetod eeldab, et vastaja – IoT tarnijad täidavad eelnevalt määratletud küsimustiku, mis hõlmab turvakontrolli, vastavust ja parimaid tavasid. Kohapealsete turvahinnangute põhjal koostatud sügava sukeldumise küsimustikud hõlmavad isiklikke hindamisi, sealhulgas rajatise ülevaatusi, intervjuusid ja süsteemiülevaatusi. Kolmandate osapoolte teenused, nagu BitSight või SecurityScoreBoard, aitavad analüüsida asjade Interneti-müüjate digitaalset jalajälge, et anda nende turvareitingud välise skannimise tulemuste põhjal.

Märksõnad: asjade internet (IoT), ohtude modelleerimine, süsteemi haavatavused, riskijuhtimine
CERCS: P170 Computer science, numerical analysis, systems, control.

Table of Contents

1. Introduction

IoT refers to the continuously expanding web of devices linked via the Internet that has made significant strides in recent years and continues to rapidly evolve. It encompasses diverse internet linked devices from wearables and smart appliances to printers, scanners, and security cameras all capable of gathering, transmitting, and responding to data. Technology has become a tool created by humans to empower people to do more and be better. Both Artificial Intelligence and IoT stand as powerful innovations that can significantly improve everyday experiences.

Many diverse industries such as finance, healthcare, agriculture, manufacturing, transportation, logistics, Oil and Gas, and others are positively transforming due to IoT implementation. AI and IoT hold transformative potential to revolutionize disaster management from prevention and mitigation to emergency response as both natural and anthropogenic catastrophes grow increasingly frequent, escalating the need for robust preparedness. IoT systems enable real-time monitoring of sudden-onset disasters like earthquakes and landslides, facilitating instant emergency alerts and seamless data transmission to command centers. This capability significantly strengthens disaster resilience by enabling proactive risk reduction and swift, data-driven crisis response [4].

The healthcare industry also benefits significantly from IoT. IoT-enabled systems allow patients and doctors to exchange data remotely, improving the efficiency of healthcare services. As global populations grow, traditional healthcare models struggle to meet demand. IoT helps reduce this burden through remote patient monitoring, telemedicine, and virtual care. Smart diagnostic tools can perform basic tests such as blood sugar level monitoring at home and send results directly to healthcare providers [1].

Like other industries, banking is also reaping the benefits of IoT. The integration of IoT technologies serves as a key catalyst for innovation in today's FinTech and banking landscape. IoT technology is changing how financial services are delivered, enhancing security, and improving efficiency. For example, IoT-powered sensors and cameras help monitor ATMs and banking infrastructure to prevent fraud, Smart ATMs send real-time data to banks for proactive cash flow and maintenance management. Banks also use IoT to track customer behavior in branches, improving service delivery and customer experience. IoT-enabled smart payment solutions significantly enhanced transactional efficiency, particularly by reducing processing times. Furthermore, these interconnected devices generate extensive customer data, including

transaction histories and behavioral insights. Through advanced analytics, FinTech firms can now discern global consumer purchasing trends. This intelligence enables financial institutions to anticipate customer needs with precision, allowing them to deliver personalized product recommendations tailored to individual financial behaviors.

Connectivity enables processes to become more efficient by allowing communication between devices, enabling automation, real-time monitoring, and remote control. The fundamental objective of IoT is to develop autonomous, interconnected devices capable of real-time communication with both users and other systems. As computer scientist Kevin Ashton articulated in 1999, IoT represents 'a network of physical objects that can exchange data independently, without requiring human interaction.

While interconnecting smart devices for data exchange and analysis revolutionizes industries, there is a downside to this progress - security issues. IoT introduces security challenges due to the lack of standardized security protocols, which can result in severe data breaches. Financial institutions, especially banks, which operate in a high-risk cybersecurity environment, become prime targets for cyber threats and face heightened risks from increasingly sophisticated attacks due to the sensitive data and financial assets they manage.

Traditional vulnerability assessment approaches are often insufficient for banking and healthcare institutions, where regulatory compliance, data privacy, and high-stakes operational integrity demand a precise and continuous assessment of vulnerabilities. Additionally, the financial and healthcare sectors' reliance on interconnected systems, third-party services, and legacy infrastructure increases the complexity of vulnerability management. A graph-based vulnerability and risk assessment model can help evaluate the impact of potential attack vectors [2].

Despite the rapid growth of IoT, statistics indicate that IoT-related vulnerabilities tend to be deprioritized compared to traditional IT vulnerabilities, even though they pose significant risks to critical infrastructure. Given the increasing adoption of IoT devices in high-risk industries, this trend presents a security gap that needs urgent attention. In order to address this challenge of vulnerability prioritization, Power BI was used to identify critical vulnerabilities in Axis and Hikvision devices — two widely used vendors in the surveillance and security industry. Power BI is a powerful tool for aggregating, analyzing, and visualizing IoT security risks. It helps organizations prioritize remediation efforts and enhance overall cybersecurity resilience.

Furthermore, Neo4j - a graph database management system was utilized to create a graph-based model that detects all vulnerable hosts in a given environment. This graph-based visualization provides a clear overview of how vulnerabilities propagate across interconnected devices, allowing organizations to map potential attack paths and mitigate threats proactively. Depicting vulnerabilities using Neo4J helps to enhance risk assessment and strengthen an organisation's security posture by providing a dynamic and adaptive visualization of its attack surface.

Integrating Power BI for vulnerability prioritization and Neo4j for attack path visualization and vendor risk assessments provides a novel approach to mitigating IoT security risks. These graph-based models offer a powerful way to assess, prioritize, and proactively address vulnerabilities, ultimately improving security in high-risk industries such as banking, healthcare, and critical infrastructure.

Beyond identifying individual vulnerabilities, evaluating a vendor's overall security posture is essential through third-party risk management (TPRM). The same Neo4j-based system was extended to assess vendor security posture across multiple lifecycle stages, incorporating such factors as Due diligence assessments, Compliance with ISO 27001 and SOC 2 standards, Self and Deep Dives assessments. This standardized process ensures organizations meet compliance requirements through systematic vendor risk evaluation and continuous supply chain security monitoring [5].

This study incorporates the MITRE ATT&CK for IoT framework to systematically evaluate threats targeting IoT devices, such as Axis surveillance cameras. This framework enabled a standardized approach to mapping vulnerabilities, for example, CVE-2021-31986 to adversarial tactics like Initial Access (T1190) and Execution (T1059). By applying ATT&CK's techniques, the research identified attack pathways unique to Axis cameras, including firmware exploits and lateral movement via RTSP protocols. The methodology not only provided a scalable security blueprint for Axis deployments but also demonstrated adaptability to other IoT ecosystems, such as medical or industrial devices. Ultimately, this structured threat analysis underscores the value of ATT&CK in unifying vulnerability management across diverse IoT environments.

While IoT technology offers transformative potential and continues to advance at an unprecedented pace, it simultaneously faces significant scrutiny across multiple dimensions. As previously discussed, the sector grapples with persistent security vulnerabilities that leave devices open to exploitation, compounded by serious privacy implications regarding data

collection and usage. Furthermore, the rapid development of IoT solutions has outpaced regulatory frameworks, creating compliance challenges for organizations. This complex landscape of innovation versus risk characterizes the current state of IoT adoption and development.

The most common IoT security issues include access control weaknesses and encryption flaws, which often lead to both home and enterprise network breaches. Compromised IoT devices serve as entry points for attackers to propagate through entire networks. Given the accelerating adoption of IoT technologies, implementing comprehensive security controls becomes increasingly critical.

Recent industry reports have underscored the critical need for robust IoT security measures. As noted in CrowdStrike's research, even a single connected device can provide cybercriminals with an initial foothold, enabling lateral network movement and potential compromise of sensitive systems [60]. Similarly, IEEE Innovation at Work emphasizes that each IoT device expands the attack surface, making security breaches more likely IEEE [61]. A study published on arXiv further outlines general attack vectors and countermeasures for securing IoT ecosystems, underscoring the need for proactive defense strategies arXiv [62].

Given this exponential expansion, based on research by Gartner, a leading provider of IT research and consulting services, there will be 29.4 billion IoT devices by 2030, and the global IoT market is expected to be worth $483 billion by 2027 therefore the need for strong IoT security measures is more critical than ever [6][48]. Proactive security measures - such as graph-based risk and vulnerability assessments as well as compliance integration (ISO 27001, SOC 2) are essential to safeguard sensitive systems in banking, healthcare, and beyond. This study bridges the gap between IoT's transformative potential and its security imperatives, offering actionable frameworks for resilient deployments.

1.1 Research Objectives

The research objectives outlined in the table below aim to systematically evaluate and enhance various aspects of IoT vulnerability management and threat modeling. The first objective focuses on assessing the role of data visualization tools, particularly Power BI, in improving risk prioritization and decision-making during IoT vulnerability remediation. This investigation seeks to determine how integrating vulnerability data with business context through Power BI can accelerate remediation efforts compared to traditional manual analysis.

The second objective examines the efficacy of remediating individual vulnerabilities within IoT ecosystems, considering their interconnected nature. This study questions whether isolated patching provides sufficient protection or if broader mitigation strategies are necessary to address systemic risks.

Another key objective explores the advantages of graph databases, such as Neo4j, in threat modeling for IoT environments. By leveraging relational data mapping, this research investigates whether Neo4j can outperform traditional linear risk models in identifying multi-stage attack paths and dynamically adapting to evolving infrastructures.

Additionally, the study aims to identify common attack paths in IoT networks that graph-based analysis can detect, particularly those involving lateral movement and protocol-based exploits.

A comparative analysis between Neo4j-based modeling and traditional STRIDE methodologies is also proposed, with a focus on dynamic IoT ecosystems like surveillance camera networks, where STRIDE's static nature may fall short.

Further objectives include investigating whether proprietary IoT protocols introduce undetected vulnerabilities that evade conventional scanning tools and developing an integrated model using Neo4j and Excel automation to dynamically aggregate vendor security posture from multiple evaluation sources. Finally, the research seeks to design a graph-based threat modeling framework combining Neo4j and MITRE ATT&CK to identify and mitigate critical attack paths in specific IoT deployments, such as Axis surveillance cameras. This framework aims to prioritize mitigation strategies based on graph-derived insights into high-risk attack vectors.

1.2 Research Questions

To address aforementioned research objectives the thesis finds answers to the following research questions (RQs):

Objective	Research Questions	Justification	Supporting Paragraph
1. To evaluate the role of data visualization tools like Power BI in enhancing risk prioritization and decision-making during IoT vulnerability remediation.	RQ1: How does risk prioritization using data visualization solutions such as Power BI improve decision-making in IoT vulnerability remediation?	Power BI integrates vulnerability data (e.g., CVSS scores, exploitability, affected hosts) with business context, enabling efficient risk prioritization. This accelerates remediation compared to manual analysis and improves decision-making in SOC teams.	Leveraging Power BI for Vulnerability Visualization and Risk Assessment in IoT Systems
2. To assess whether remediating single vulnerabilities is an effective strategy within the broader context of IoT ecosystem security.	RQ2: Is remediation of single vulnerabilities a recommended approach for IoT ecosystems?	IoT systems are interdependent, and patching isolated vulnerabilities may not provide comprehensive protection. This study evaluates whether broader mitigation strategies are more effective for systemic risk reduction.	Leveraging Power BI for Vulnerability Visualization and Risk Assessment in IoT Systems
3. To explore how graph databases such as Neo4j enhance threat modeling through relational data mapping compared to linear risk models.	RQ3: How can graph databases such as Neo4j improve threat modeling for IoT ecosystems compared to traditional linear risk assessment methods?	Neo4j captures relationships between devices to reveal multi-stage attack paths often missed by linear models. It dynamically adapts to evolving infrastructures, enhancing visibility into systemic vulnerabilities in environments like camera networks.	Introduction to Graph Theory in Cybersecurity through Neo4j Threat Modeling for IoT (Axis Cameras) Using MITRE ATT&CK & Neo4j

4. To identify common attack paths in IoT networks that graph databases can detect through relationship-based threat modeling.	RQ4: What are the most common attack paths in IoT networks that Neo4j can identify through relationship-based analysis?	Neo4j uncovers hidden attack vectors by linking devices and exploits in real time. This highlights critical risks such as lateral movement via SMBv1 and enables preemptive defenses against cascading breaches.	Common IoT Vulnerabilities and Exploits Leveraging Neo4J for Vulnerability Assessment
5. To compare Neo4j-based modeling with traditional STRIDE methodologies, particularly in dynamic IoT ecosystems like surveillance camera networks.	RQ5: What limitations make STRIDE less effective for threat modeling in large-scale, dynamic IoT environments such as Axis camera networks, particularly in identifying runtime threats like wormable SMBv1 exploits?	STRIDE is static and asset-focused, struggling with dynamic IoT systems and runtime threats. It lacks scalability, automation, and support for proprietary protocols, making it less effective in complex deployments.	STRIDE – Threat Modeling Framework
6. To determine if proprietary IoT protocols introduce hidden vulnerabilities that evade traditional vulnerability scanners.	RQ6: Do proprietary IoT protocols increase undetected vulnerabilities in traditional scanners?	Non-IP protocols like Zigbee and MQTT often bypass tools like Nmap or Nessus, increasing the risk of unaddressed vulnerabilities, especially in firmware or services like SMBv1.	Limitations of Traditional Scanning and the Need for Adaptive IoT Security Approach
7. To design an integrated model using Neo4j and Excel automation for dynamically aggregating vendor security posture from multiple evaluation sources.	RQ7: How can organizations leverage Neo4j and Excel automation to aggregate and visualize a comprehensive and dynamic Security Posture for vendors, by integrating multiple security evaluations such as due diligence questionnaires, self-assessments, deep dives, and vulnerability scans?	Neo4j can consolidate and model diverse vendor evaluations to generate a dynamic, visual representation of third-party risk posture. Excel forms can be automated for streamlined integration.	Evaluating IoT Suppliers from a TPRM Perspective How Graph Databases Neo4j Can Enhance Third-Party Risk Management Program Analysis

8. To develop a graph-based threat modeling framework using Neo4j and MITRE ATT&CK for IoT that identifies and mitigates critical attack paths in Axis surveillance camera networks.	RQ8: How does Neo4j's relationship-based analysis reveal high-risk attack paths in Axis cameras that traditional linear threat models overlook? RQ9: What mitigation strategies are most effective in disrupting identified attack paths, and how can they be prioritized using graph-derived insight?	Neo4j, paired with MITRE ATT&CK, provides deep visibility into high-risk vectors like default credentials and firmware exploits. Graph-based analysis helps prioritize effective mitigations through attack path mapping.	Threat Modeling for IoT (Axis Cameras) Using MITRE ATT&CK & Neo4j

1.3 Target Audience

Attack graphs play a critical role in mitigating multi-step attacks by illustrating all possible sequences of vulnerabilities and their interdependencies. These graphs serve as valuable tools for identifying security weaknesses and generating recommendations to strengthen network nodes against potential exploits. In cybersecurity, attack graphs are used to assess whether an attacker can achieve a specific goal when attempting to infiltrate a network from an initial starting position. In this context, they represent an attacker's actions and the resulting changes in the network state. The starting node signifies the attacker's initial location within the network, while nodes and arcs depict the attacker's steps and the impact of their actions. These actions often involve exploiting software or protocol vulnerabilities to escalate privileges on one or more target systems, which could include user devices, routers, firewalls, or other critical network components.

In complex attack scenarios, multiple steps may be necessary to compromise intermediary hosts and use them as pivot points to reach the ultimate target. An attack graph provides a complete visualization of all possible attack sequences that could lead to a specific privilege escalation on a system. Different modeling approaches exist: some frameworks define nodes as system states and edges as attack steps, whereas others treat both states and actions as nodes or represent actions as nodes connected by state transitions. Additionally, attack graphs can vary in complexity, with some featuring a single attacker starting position and a single target, while others account for multiple attackers originating from different locations within the network [35].

Given the technical nature of attack graphs and their role in cybersecurity, the primary target audience for this research includes cybersecurity researchers and academics, as attack graphs are widely studied in academia to model and analyze security threats. Researchers in network security, cyber threat intelligence, and security analytics will benefit from understanding how attack graphs can predict multi-step attacks, particularly when enhanced by integrating MITRE ATT&CK frameworks within Neo4j to map adversary tactics and techniques, thereby creating full attack chains for more effective vulnerability mitigation. This approach is also valuable for professionals responsible for Security Operations Center (SOC) activities, penetration testing, and incident response, as it enables more precise adversary emulation and threat modeling. Additionally, Third-Party Risk Management (TPRM) teams and vendor security assessors can leverage these methodologies to evaluate supply chain risks and enhance vendor security postures through dynamic, relationship-based analysis. Relevant disciplines such as computer science, information security, and cybersecurity engineering will find this research applicable, as it bridges theoretical attack graph models with practical implementations in IoT ecosystems and enterprise security frameworks.

2. IoT Devices, Architecture and Components

The Internet of Things (IoT) represents a fundamental shift in how devices, systems, and people interact, creating smart ecosystems that enhance automation, efficiency, and decision-making. However, the distributed and heterogeneous nature of IoT introduces significant security challenges. Unlike traditional IT systems, IoT architectures span multiple layers from edge devices to cloud-based analytics each with unique vulnerabilities. Securing IoT requires a holistic approach, addressing not just individual weaknesses but the entire attack surface, including device integrity, network security, data protection, and third-party risks.

Understanding the complexity of IoT systems is crucial before conducting any threat and vulnerability assessments. The threat landscape, risk models, and attack vectors vary based on the IoT category segment. The context, stakeholders, and vulnerabilities differ significantly across different segments, making it essential to distinguish between Business-to-Consumer (B2C) IoT (smart home devices, wearables) and Business-to-Business (B2B) IoT (industrial, enterprise, healthcare systems). While B2B cybersecurity focuses on protecting business data and maintaining enterprise trust, B2C cybersecurity prioritizes consumer privacy and regulatory compliance. Both sectors require tailored security approaches to mitigate risks in an increasingly hostile cyber landscape.

At the foundation of IoT systems lie the physical components that interact with the real-world sensors that detect environmental changes, actuators that perform physical actions, and embedded systems that process and transmit this data. These fundamental elements typically have constrained processing capabilities, which presents significant challenges for implementing comprehensive security protections. The limitations in computing resources often force compromises in security implementations, leaving systems vulnerable to exploitation. Malicious actors frequently target these weaknesses through various means including bypassing authentication protocols, physically manipulating device hardware, or capturing unprotected data transmissions. Each of these attack vectors poses serious risks, as compromising just one of these foundational components can potentially undermine the security of the entire interconnected system. The nature of these devices being deployed in often unprotected physical environments further compounds these security challenges, requiring careful consideration of both digital and physical protection mechanisms [59].

The Connectivity Layer facilitates communication between devices and gateways using protocols like Wi-Fi, Bluetooth, LPWAN, and cellular networks. Each of these technologies

has its own security limitations Bluetooth may be susceptible to sniffing, while unsecured LoRaWAN gateways can be hijacked. Man-in-the-middle attacks, rogue device impersonation, and protocol vulnerabilities are common threats at this stage. Ensuring encrypted transmissions, mutual authentication, and intrusion detection is critical to maintaining trust in IoT networks.

Once data is collected, it moves through Edge Computing nodes, which preprocess information before sending it to the cloud. These gateways are prime targets for attackers, as compromising them can allow manipulation of data streams or unauthorized access to backend systems. Secure firmware updates, hardware-based root-of-trust mechanisms, and runtime integrity checks are essential to protect these critical junctions [15].

The Data Accumulation and Abstraction Layer stores and normalizes incoming data for analysis. Cloud-based storage and processing introduce risks such as unauthorized access, data breaches, and injection attacks. Strong encryption (both at rest and in transit), strict access controls, and anomaly detection systems help mitigate these threats. Additionally, privacy-preserving techniques like differential privacy can prevent sensitive information from being exposed.

At the Application Layer, user-facing services such as smart home dashboards or industrial monitoring systems must enforce strict authentication and authorization. Weak access controls, insecure APIs, and improper session management can lead to account takeovers or data leaks. Role-based access, multi-factor authentication, and continuous security testing are necessary to safeguard applications.

Finally, the Collaboration and Processes Layer integrates IoT insights into business workflows, often relying on third-party services. Supply chain risks, insecure vendor integrations, and compliance gaps can introduce vulnerabilities. Organizations must conduct thorough security assessments of external partners, enforce contractual security obligations, and monitor for anomalies in third-party interactions.

From a business standpoint, IoT products are segmented into four key components:

- Hardware-Defined Product (HDP) – Includes sensors, actuators, and embedded systems that capture and transmit data.
- Network Fabric – Connects hardware to software components.

- Software-Defined Product (SDP) – The "brain" of IoT, consisting of a Cyber Model (digital twin) and Application (user/data interface).
- External Systems – Integrates with broader enterprise or consumer ecosystems.

The Software-Defined Product (SDP) is central to IoT value creation, acting as a virtual representation of the physical product. It processes data from sensors, runs analytics, and enables intelligent decision-making. The Cyber Model (or digital twin) simulates real-world behavior, while the Application orchestrates interactions between users, data sources, and external systems [71].

Given the vast number and diversity of IoT devices, securing each component individually is impractical. Instead, organizations should adopt a Third-Party Risk Management (TPRM) approach, ensuring vendors adhere to strict security standards, which include: vendor security assessments - evaluating suppliers' security posture before integration; contractual security obligations - enforcing encryption, patch management, and compliance requirements; and continuous monitoring - detecting anomalies in third-party services. TPRM will be reviewed in more detail further down in the thesis, where the author will also introduce the proposed framework.

IoT's complexity demands a defense-in-depth strategy, combining strong encryption (AES, ECC), secure communication (TLS/IPSec), access controls, and continuous monitoring. As IoT adoption grows, so will the sophistication of attacks. Proactive security practices, threat intelligence, and adaptive defenses are crucial to safeguarding the interconnected future. By embedding security at every layer from hardware to cloud and holding third parties accountable, organizations can build resilient IoT ecosystems capable of withstanding evolving threats.

2.1 IoT Security Challenges and Risks

The major security risks in IoT stem from device vulnerabilities, data breaches, unsecured communications, and privacy threats. To counter these risks, communication channels must be properly authenticated to block unauthorized access while ensuring privacy to prevent intruders from eavesdropping or stealing sensitive data.

Current IoT security challenges include the widespread use of default or weak passwords, insufficient privilege management, and an expansive attack surface due to insecure open ports.

Outdated firmware, software, and operating systems further exacerbate risks, along with weak or missing encryption for stored and transmitted data. Inadequate authentication and authorization mechanisms, software bugs, lack of digital signatures, and poor physical security protections for individual devices also leave IoT systems exposed to exploitation. Addressing these weaknesses is essential to building a more secure IoT ecosystem.

Every device that needs internet access, must run over an operating system. Day by day every operating system strengthens its security to fight against known vulnerabilities. So new versions are also released with necessary updates. But IoT devices, once set up, are hardly being updated to new releases of operating systems. This opens up a space to attackers to make the system attack easily. Though the devices run an operating system, the underlying hardware specification is not that great to run an antivirus application like any other desktop computers. This increases the chance of attack by malwares which attack systems and steal sensitive data.

Another problem of having low end specifications is application update. Application softwares is developed in the latest high end systems, though they are used in various scales of devices. Generally passwords are used as initial restrictions of IoT devices. Manufacturers by default set a password to that device. But they do not satisfy the latest security standards because those passwords are set up for demonstration whereas users most of the time use that default password as a regular one. Thus this increases the probability of guessing the passwords by the attackers.Most of the IoT devices are designed to be used in public places, like CCTV cameras. In those cases, the security needs to be well planned so that any attacker cannot bypass the existing security walls to gain access to that device.

Internet protocols are implemented to gain a layer of security when communicating between nodes over the internet. There are many protocols designed, some of them are deprecated also, like Telnet, because of its lack of built in security. But devices are well known for using these protocols for simplicity. IoT devices may seem harmless, but they can be a critical entry point for attackers.

Such devices as printers and CCTV cameras that are connected to the network often lack strict security protocols and use default credentials. Even when default credentials are changed, they are often easy to crack due to poor practises like weak password selection, credential sharing or reuse or infrequent rotation. By leveraging these credentials attackers can access vulnerabilities in IoT system software and perform a lateral movement to get deeper into company systems and supply chains [12]. To advance this research, we will examine statistics

reflecting high-ranking managers' perspectives on security maturity, along with projected numbers of potential future attacks based on their responses.

In 2017, the Ponemon Institute, sponsored by Shared Assessments, conducted a study titled A New Era of Third-Party Risks to assess organizations' awareness and preparedness for the emerging enterprise IoT landscape. The research surveyed 553 professionals involved in risk management, all of whom were familiar with IoT applications and their associated risks within their organizations. Despite this awareness, the study revealed that efforts to mitigate third-party risks in the IoT ecosystem were inadequate. The primary obstacles to addressing these risks were a lack of organizational prioritization and insufficient allocated resources. [13].

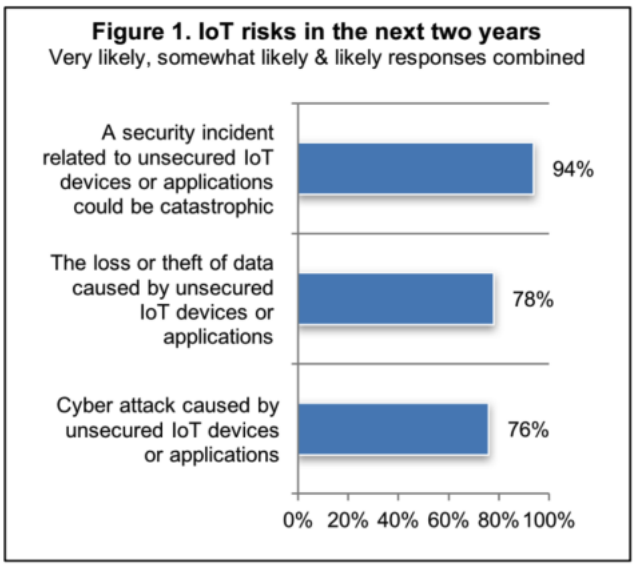

Figure 1. IoT Risks in the next two years [14]

Based on a New Era of Third-Party Risks sponsored by Shared Assessments it has been identified that the percentage on IoT risks mitigation is relatively low. As can be seen in Figure 2 the responses are pessimistic about their ability to minimize IoT risks and avoid attacks.

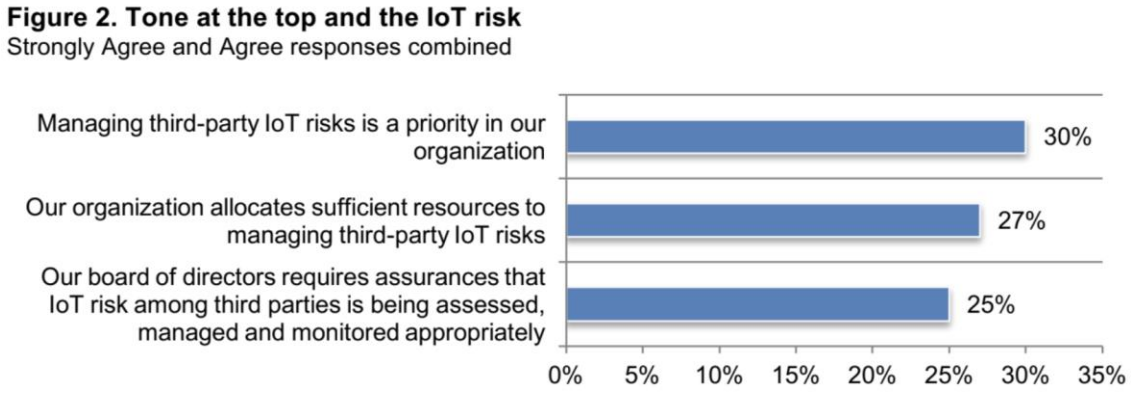

Figure 2. IoT risk management

In addition, NetGear report reveals the following information on IoT Security Landscape:

- Every 24 hours, home network devices see an average of 10 attacks.
- Every 24 hours, Bitdefender smart home security solutions block an average of 2.5 million threats, or roughly 1,736 threats per minute [15].

Based on the above statistical reports, it can be concluded that IoT attacks are expected to continue increasing in both frequency and sophistication as companies continue to incorporate Internet of Things projects into their business or are planning to work with IoT in the upcoming years. Besides relatively low percentage on IoT risks mitigation and high potential of security breaches in the upcoming years there is another challenge related to IoT such as high-rank talent and expertise in the IoT sphere is scarce which would lead to the fact that most companies in order to stay cost efficient will be outsourcing IoT services instead of building an internal team of developers. Outsourcing IoT operations shifts security responsibilities to companies, requiring them to verify that all their third-party vendors maintain rigorous security protocols. This is particularly crucial as modern organizations depend heavily on external providers for mission-critical business functions. The growing reliance on outsourced services makes comprehensive vendor security assessments an essential component of any IoT deployment strategy. On average, organizations share sensitive data with approximately 583 external vendors [13].

Another challenge is that while multiple security frameworks and standards exist for IoT, there is no unified approach that comprehensively addresses security implementation regardless of whether an organization is procuring IoT services/devices or manufacturing them. There are various guidelines that have emerged to tackle IoT security, including NISTIR 8259, which establishes a secure-by-design baseline for manufacturers [26]; the IoT Security Foundation (IoTSF), offering best practice guidance for manufacturers and users [27]; ETSI EN 303 645, setting baseline security requirements for consumer IoT devices [28]; OWASP IoT Security, which identifies common risks and best practices [29]; and the Industrial Internet Consortium (IIC) Security Framework, focusing on industrial and critical infrastructure IoT security [30]. These frameworks can be applied individually or combined based on industry and regulatory needs, providing structured methodologies for threat identification, assessment, and mitigation. Additionally, reference architectures like the IIC's Reference Architecture and accompanying Industrial Internet Security Framework (IISF) [32] support large-scale IoT security implementations. However, these frameworks primarily outline risk management conditions without detailing specific risk analysis or assessment methods, leading to inconsistencies in evaluations and making cross-framework comparisons difficult [37]. While effective for traditional security risks, they fall short in addressing modern IoT systems, which introduce cyber-physical assets and complex interdependencies. Conventional IT risk assessment methods struggle with IoT's scale, density, and dynamic nature, necessitating continuous rather than periodic evaluations.

IoT's interconnectedness evident in industrial supply chains which means an asset's risk depends on linked devices, requiring assessments to account for cascading effects. Furthermore, IoT systems merge cyber and physical components, demanding risk models that evaluate combined attack vectors, where threats against physical assets can lead to cyber compromises and vice versa. The complexity of these interdependencies complicates risk management, particularly in integrating communication, computing, and control technologies. Effective risk assessment also relies on comprehensive Security Knowledge Bases (SKBs) or Configuration Management Databases (CMDBs). Yet, IoT systems demand far more sophisticated knowledge than conventional IT systems not just device vulnerabilities but also how risks propagate across connected assets. Traditional knowledge bases often prove inadequate, increasing the likelihood of overlooked risks and errors in assessment.

2.2 Rising Security Threats Due to Growth of IoT

Security awareness often gains prominence in the aftermath of significant incidents. The research is motivated by real-world examples where IoT devices were compromised, resulting in substantial impacts. Such experiences underscore the critical need to enhance our understanding of IoT risks and develop more effective strategies to mitigate them. Mirai Botnet, VPNFilter, BrickerBot, Persirai Botnet attacks are examples of most sophisticated attacks on IoT devices [73,74,75,76,77].

Table 1. Most sophisticated attacks on IoT devices and it's impact

Attack Name	Year	Target	Method	Impact
Mirai Botnet	2016	IoT devices (cameras, routers, etc.)	Exploited default credentials to build a botnet for DDoS attacks	Took down major websites (e.g., Twitter, Netflix, Reddit) via Dyn DNS provider
Mozi Botnet	2019	IoT devices (routers, DVRs, etc.)	Used Telnet brute force and known exploits	Created a large P2P botnet, sustained DDoS attacks
VPNFilter	2018	Routers and network-attached storage	Multi-stage malware; exploited known router vulnerabilities	Affected over 500,000 devices globally
BrickerBot	2017	Insecure IoT devices	Permanent Denial of Service (PDoS) – corrupts device storage	Bricked thousands of IoT devices, rendering them unusable
Persirai Botnet	2017	IP Cameras	Exploited known vulnerabilities in Chinese-made cameras	Infected over 120,000 cameras globally
Raptor Train IoT Botnet	2024	Routers and IP cameras	The botnet spreads by exploiting unpatched vulnerabilities in IoT devices	200,000 devices worldwide compromised
Matrix Botnet	November, 2024		IoT devices turned into a global botnet used to carry out distributed denial-of-service (DDoS) attacks. IP ranges of several cloud service providers for IoT were scanned to identify unpatched vulnerabilities and misconfigurations.	Up to 35 million of potential devices affected

The widespread integration into modern life often occurs without consistent security measures, embedding vulnerabilities across homes, offices, factories, and hospitals. The disruptive potential of these vulnerabilities was starkly demonstrated on October 21, 2016, when the Mirai botnet launched a massive attack against DYN, a major DNS provider. The assault disrupted services for prominent platforms like Twitter, Reddit, Airbnb, and Netflix, affecting users across North America and Europe with outages and slowdowns. Reaching 1.2 terabits per second, it became one of the largest DDoS attacks ever recorded, exposing the alarming power of IoT-based botnets and the critical need for stronger security measures. The Mirai attack, is one of the most significant incidents involving IoT devices, had profound global impact, underscoring the vulnerabilities inherent in such systems. This event served as a catalyst for heightened awareness of IoT security, elevating it to a critical concern for organizations, governments, and individuals. The Mirai attack revealed fundamental weaknesses in IoT security, as many manufacturers shipped devices with default credentials, weak update mechanisms, and limited user controls, making them easy targets for exploitation. It was created to exploit IoT devices such as IP cameras, routers, DVRs by scanning the internet for devices with default factory settings and hard-coded usernames and passwords like admin and 12345. Mirai easily compromised these vulnerable systems. Once infected these devices would report back to a command and control CNC server creating a self-propagating network of compromised devices known as a botnet. The primary weapon in Mirai arsenal was the distributed denial of service DOS attack. By overwhelming a target server or network with a flood of internet traffic Mirai could render services unusable. The sheer size of the botnet and the bandwidth capabilities of the infected IoT devices made these attacks incredibly potent [73,123].

In its aftermath, there was a concerted push for improved IoT security standards, with governments and regulatory bodies exploring mandates for unique default passwords, automatic updates, and better device hardening. The incident also raised awareness among consumers and businesses, prompting recommendations to change default credentials, maintain firmware updates, and segment IoT devices on isolated networks to reduce exposure. Together, these cases underscore how ransomware and botnet threats exploit IoT's unique risks spanning insecure device proliferation, supply chain flaws, and the challenges of securing embedded systems while highlighting the urgent need for comprehensive security frameworks [73].

Malware or malicious software represents the most prevalent form of cyberattack, largely because it includes a wide range of subtypes such as ransomware, trojans, spyware, viruses,

worms, keyloggers, bots, and cryptojacking. Ransomware, a particularly disruptive category, manifests in two primary forms: locker ransomware, which blocks access to a system by locking the user interface, and crypto-ransomware, which encrypts files using sophisticated algorithms. More advanced variants extend their reach beyond local systems, targeting hard drives, databases, backups, USB storage, and even cloud-based data. In both cases, attackers demand payment typically in cryptocurrencies like Bitcoin to restore access to the compromised systems or files.
[124].

The 2024 SonicWall Cyber Threat Report was published by Cyber Management Alliance Ltd., a globally recognized cybersecurity consultancy and training provider headquartered in London, UK, noted an approximate 107% surge in IoT malware attacks during the year. Recent industry reports highlight escalating cyber threats across multiple fronts. Sophos' The State of Ransomware 2024 reveals that 59% of surveyed organizations experienced ransomware attacks. Meanwhile, phishing incidents surged by 4,151% following ChatGPT's public release, as documented in SlashNext's The State of Phishing 2024. Distributed denial-of-service (DDoS) attacks also proliferated, with Netscout detecting approximately 8 million incidents in the first half of 2024. According to IBM and the Ponemon Institute, the financial impact remains severe, with the average data breach costing organizations $4.88 million this year. [125].

There are several IoT Ransomware Attack Types targeting IoT ecosystems specifically. First are device hijacking attacks where threat actors compromise IoT devices to create botnets for large-scale attacks like DDoS campaigns. Second is data encryption ransomware that specifically targets sensitive information collected by IoT devices such as medical records or surveillance footage. Third are device lockout attacks that render IoT controllers or smart home systems inaccessible until ransom is paid. Fourth are hybrid attacks combining data encryption with device functionality manipulation, such as tampering with industrial sensors or disabling security cameras. Fifth are supply chain attacks compromising IoT devices during manufacturing or software updates to deploy ransomware later. And emerging AI-powered ransomware that adapts to bypass IoT security measures through machine learning [123].

The growing sophistication of IoT ransomware, ranging from device hijacking to AI-adaptive variants, demands comprehensive defense strategies combining technical controls, regulatory frameworks, TPRM and advanced analytics. While there is still no single solution that would provide a complete protection, the need for continued research into adaptive graph techniques

capable of handling IoT's unique characteristics, as well as greater collaboration between manufacturers and security researchers to develop standardized defense frameworks for the evolving IoT threat landscape persist [123].

3. Common IoT Vulnerabilities and Exploits

The Open Web Application Security Project (OWASP) has systematically identified critical vulnerabilities affecting IoT ecosystems through rigorous analysis of real-world deployment scenarios. Their research methodology, grounded in empirical study of operational IoT systems, reveals fundamental security weaknesses that jeopardize device integrity and ecosystem security.

A particularly pervasive vulnerability stems from inadequate authentication practices. Numerous IoT devices remain susceptible to compromise due to three interrelated factors: the persistence of default manufacturer credentials, the prevalence of easily guessable passwords, and the continued use of hard-coded authentication strings. These authentication failures create low-barrier entry points for malicious actors, as end users frequently fail to modify the insecure default configurations provided with devices. This systemic issue underscores the ongoing challenges in establishing basic security hygiene across IoT deployments.

These hardcoded passwords can be exploited by automated scripts and bots. Insecure network services further worsen the situation by exposing unnecessary ports and services to the internet. These services often lack proper authentication or encryption. As a result, attackers can easily intercept or manipulate data. Insecure ecosystem interfaces, including mobile apps and cloud services, are also common attack vectors. These interfaces may not properly validate input or may expose sensitive APIs. Without proper security checks, attackers can gain control over the device or its data. Insecure software patching capabilities represent another major weakness. IoT devices must be regularly patched to fix known bugs and security issues. Without secure updates, devices remain exposed to known exploits. Some devices even allow unsigned firmware updates, which can be hijacked by malicious actors. Using insecure or outdated components increases the attack surface. Many IoT products rely on open-source libraries with known vulnerabilities. These components are often overlooked during development. Insecure data transfer and storage mean that sensitive information like passwords or location data can be exposed. When encryption is not used, it becomes easy to intercept and steal data. Lack of data protection can lead to privacy violations and identity theft. The absence of device management further complicates things. Organizations can’t monitor, configure, or update their devices efficiently without proper management. This makes it harder to detect or respond to attacks. Insecure default settings make devices vulnerable out-of-the-box. Many users are unaware of these defaults and never change them. This gives attackers a consistent way to exploit devices. Lack of physical hardening is another overlooked area. When physical device

access is obtained, malicious actors can both retrieve stored information and deploy harmful firmware modifications. Devices must be built with tamper resistance in mind. Physical ports should be secured or disabled if not needed. Overall, IoT security must be prioritized to prevent these vulnerabilities from being exploited. Developers, manufacturers, and users all have a role in securing the IoT ecosystem. Without strong security practices, these devices can pose serious threats to individuals and organizations alike. Addressing these issues is crucial as IoT adoption continues to grow. Only with comprehensive security can we truly benefit from the potential of IoT [80].

The inherent vulnerabilities in IoT devices make them prime targets for botnet recruitment, particularly for orchestrating distributed denial-of-service (DDoS) attacks. This was starkly demonstrated in 2016 when the Mirai botnet infected more than 600,000 IoT devices primarily routers and surveillance cameras to execute a record-breaking DDoS attack that reached 620 gigabits per second at its peak. Since then, new strains of malware have emerged, introducing more sophisticated and multifaceted attack methods.The Xbash malware combines botnet capabilities with ransomware, cryptomining, and self-propagation. It is particularly destructive, targeting Linux and Microsoft Windows servers by exploiting weak passwords and unpatched vulnerabilities. Similarly, a recent variant of the Muhstik botnet autonomously installs itself on Linux servers and IoT devices, spreading like a worm to facilitate crypto mining and DDoS attacks [73].

To understand these attacks and their impact, it is crucial to examine the attack surfaces of IoT devices, which fall into three main categories: hardware interfaces - the physical components of an IoT device present an obvious attack vector. By accessing the device's outer shell or operating system kernel, attackers can manipulate firmware, embed backdoors, and bypass authentication mechanisms. Communication channels, as IoT devices rely on various communication protocols, including short-range channels like BLE, Zigbee/Z-Wave, and Wi-Fi, as well as long-range cellular networks. The absence of robust encryption protocols during IoT device provisioning creates multiple attack vectors, leaving systems exposed to IP spoofing, interception attacks, message replay exploits, and service disruption attempt. And applications/services which is one of the most targeted attack surfaces due to its scalability and accessibility. Web APIs, cloud servers, administrative interfaces, and system functionality components can all be exploited. Attackers frequently compromise IoT services to infiltrate enterprise networks, even if they are deployed on an intranet. For example, the Xbash botnet can penetrate enterprise intranets to scan and attack various services, such as Telnet and FTP [36].

3.1 Limitations of Traditional Scanning and The Need for Adaptive IoT Security Approaches

There is a wide range of vulnerability scanners available, designed to automatically detect security flaws in IT systems. Both commercial and open-source options exist, each with its own advantages and limitations [104]. Contemporary vulnerability scanning solutions predominantly depend on established security classification standards, including the Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), and Common Vulnerabilities and Exposures (CVE) list, to systematically evaluate and classify security risks. As the most prevalent assessment framework, CVSS serves as the foundation for the U.S. National Vulnerability Database's (NVD) vulnerability severity evaluations. The CVSS methodology employs a comprehensive three-tiered scoring approach consisting of Base, Temporal, and Environmental metrics. The Base metric establishes a fundamental severity rating on a scale from 0 to 10, which can then be refined through Temporal metrics that account for changing threat conditions, or Environmental metrics that incorporate organization-specific operational contexts and mitigation factors. While CVSS v2 and v3 remain prevalent, the newer v4.0 offers refined scoring. These scores are typically computed using the NVD’s online calculator. Complementing CVSS, CWE provides a taxonomy of software weaknesses, helping identify root causes of vulnerabilities, while CVE serves as a universal identifier for known security flaws, enabling consistent tracking and remediation across tools and platforms. Together, these frameworks form the backbone of modern vulnerability assessment, allowing scanners to prioritize and mitigate risks systematically [114, 115]. There are several world-known IoT vulnerability scanning solutions that are able to identify vulnerabilities in IoT devices depending on its type, such as OpenVAS, Nessus, Burp Suite, Qualys, Kaspersky's IoT Security Scanner, Shodan as well as Cisco's IoT Threat Defense.

Conventional network scanning tools frequently prove inadequate for detecting and protecting IoT devices, owing to the distinct architectural and operational characteristics inherent to these connected technologies. Many IoT devices do not rely on standard IP-based communication, instead, they use lightweight or proprietary protocols such as Bluetooth, Zigbee, Z-Wave, MQTT, or CoAP. As a result, scanners like Nmap or even more advanced vulnerability scanners like Nessus may fail to detect these devices or misidentify their behavior. This

limitation becomes particularly critical when devices operate without a traditional IP address or rely on multicast and low-power wireless communications [103].
When IoT devices are IP-based, such as network surveillance cameras from manufacturers like Axis, tools like Nessus can be effectively used to scan and detect vulnerabilities. These devices respond to typical network protocols like HTTP, RTSP, or SNMP, which are easily handled by conventional scanning tools. Nessus and similar scanners can assess the configuration, detect outdated firmware, and flag open ports or weak credentials. However, this approach is viable primarily when the IoT devices adhere to familiar IP-based networking models.
In cases where devices are non-IP-based or communicate over typical protocols, graph-based assessment models offer a more suitable approach. These models map out communication patterns, device behaviors, and network relationships to infer the presence and risk profile of IoT endpoints. Instead of relying solely on IP scanning, graph models use behavior correlation, passive monitoring, and traffic analysis to identify anomalies and unknown devices, which is essential in environments dense with IoT systems that traditional scanners miss [103].

The complex interactions between IoT components create unique security considerations. These devices operate through interdependent relationships, requiring both secure controller communications and mutual dependencies established through application-level connections or physical interfaces. This distributed yet interconnected architecture presents significant obstacles for complete security evaluation and vulnerability analysis [105], [106], [107], [108], [109]. Merely securing individual elements or select groups of components proves inadequate for protecting the entire system, as adversaries can exploit various attack vectors to access critical resources. A case in point involves smart door security: while attackers could directly target vulnerabilities in the locking mechanism [110], they might alternatively compromise a connected indoor camera [111] to deliver fabricated audio commands that manipulate a smart speaker into opening the door.

Consequently, effective IoT protection necessitates a multifaceted methodology that integrates traditional IP-based scanning tools with passive monitoring solutions for non-IP devices, complemented by CVSS-based risk evaluation. To ensure complete ecosystem security, this approach must incorporate segmented network architectures, persistent surveillance mechanisms, systematic firmware maintenance, and purpose-built IoT security solutions that provide end-to-end oversight.

Attack graphs provide an elegant approach to analyzing potential attack paths by enumerating all possible routes to critical system goals [117], [118], [119]. These models fall into two categories: state-based attack graphs[118], which use model checking but suffer from scalability issues due to exponential growth with system state variables (a linear function of device count), and exploit-dependency attack graphs[117], [119], which are more efficient, requiring only polynomial time for construction while scaling quadratically with device count. However, it is important to consider that an exploit-dependency attack graphs face significant limitations in IoT environments due to the prevalence of low-level, non-standard communication protocols, as it has been discussed earlier, such as Zigbee, Z-Wave, BLE, and MQTT [103]. Unlike conventional networks, IoT ecosystems often rely on proprietary, event-driven, or power-efficient protocols that lack the transparency of traditional TCP/IP-based systems. This makes it difficult to model attack paths accurately, as many IoT devices bypass standard authentication, use weak encryption, or operate without proper session management factors that conventional attack graphs fail to capture.

Additionally, IoT networks are highly dynamic, with devices frequently entering sleep modes, forming ad-hoc connections, or interacting unpredictably across manufacturers. This instability leads to incomplete attack path predictions, as traditional exploit-dependency models assume stable topologies. Furthermore, these frameworks depend on known CVEs and patch-based assessments, while many IoT devices run on unpatched or undisclosed firmware vulnerabilities. The absence of standardized security controls in low-level protocols further complicates modeling efforts.

Given these challenges, a comprehensive IoT security strategy must combine both attack graph models and hybrid scanning techniques to effectively mitigate risks. While exploit-dependency graphs offer structured threat analysis for conventional networks, IoT environments demand adaptive approaches that account for physical dependencies, intermittent communications, and protocol-specific weaknesses. Integrating behavioral monitoring, network segmentation, and specialized IoT security platforms with these models can enhance visibility and control, ensuring a more robust defense against evolving threats.

3.2 Vulnerability Scanning Vendor – Tenable, Nessus Scanner

This section explores the capabilities of Nessus Scanner in the context of IoT security. Moving forward, Nessus will continue to be utilized for traditional vulnerability scanning of IP-based IoT devices, leveraging its ability to automatically discover and identify connected devices including those that might otherwise remain undetected. The scanner adopts a risk-based approach to vulnerability management, enabling prioritization based on potential impact.
Tenable maintains an open-source plugin database (https://www.tenable.com/plugins), which later in the research will be leveraged to construct a vulnerability prioritization graph for surveillance camera systems from prominent vendors like Axis, Hikvision, and Mobotix. The objective is to visualize and prioritize high-severity vulnerabilities for remediation. Nessus plugins are designed to detect specific vulnerabilities, misconfigurations, and compliance issues, drawing from multiple sources including public vulnerability databases (CVE, CVSS), vendor advisories, threat intelligence feeds, and Tenable's proprietary research.

IoT systems, in particular, exhibit a high density of security vulnerabilities. While responsible disclosure has traditionally been the norm, this approach struggles to keep pace with the rapid evolution of IoT, a domain characterized by cost constraints, long lifespans, and dynamic threat landscapes [17]. Tenable plugin development often depends on vendor cooperation for technical details and patches before public disclosure. Regulatory shifts, such as the UK's Product Security and Telecommunications Infrastructure (PSTI) legislation enforced from April 29, 2024 now mandate coordinated vulnerability disclosure (CVD) for consumer IoT manufacturers, reinforcing the need for structured vulnerability management in this space.

Tenable provides an open source database https://www.tenable.com/plugins which will be used in this paragraph to build a graph based vulnerability prioritisation graph using Tenable plugins to evaluate the risk associated with surveillance camera systems from well-known vendors such as Axis, Hikvision and Mobotix. The main goal of the graph is to visualize and help to prioritize vulnerabilities associated with surveillance camera systems and its prioritization for remediation of the vulnerabilities that have high severity scores. Nessus plugins are files that are built to detect specific vulnerabilities, configurations, and compliance issues within the IT environment. They are primarily designed for use with Nessus, Tenable.sc, and Tenable.io to automate vulnerability and compliance scans. Each plugin is based on data from multiple sources, including:

- Publicly available vulnerability databases (CVE, CVSS, etc.)
- Vendor-specific advisories and patch notes
- Industry threat intelligence feeds
- Custom research from Tenable own security teams

All technological systems contain security vulnerabilities, but IoT solutions present particularly numerous exposure points. While responsible disclosure has long served as the security community's standard practice for addressing discovered vulnerabilities, this methodology struggles to adapt to today's rapid development cycles. The challenges are especially pronounced in the IoT domain, where devices typically combine low production costs, limited hardware resources, extended operational lifespans, and constantly evolving threat landscapes [17].

While creating its own vulnerability detection plugins, Tenable often relies on vendors to provide technical details, patches, or mitigation guidance before publicly disclosing vulnerabilities. Recent developments indicate that vulnerability disclosure is becoming a mandatory requirement for IoT vendors particularly in the consumer sector. The UK's Product Security and Telecommunications Infrastructure (PSTI) legislation, effective from April 29, 2024 mandates that consumer IoT device manufactures implement coordinated vulnerability disclosure policies (CVD).

3.3 Leveraging Power BI for Vulnerability Visualization and Risk Assessment in IoT systems

Microsoft Power BI is a cloud-based Software-as-a-Service (SaaS) platform that enables organizations to develop comprehensive business intelligence solutions. The service provides capabilities for creating interactive dashboards, analytical reports, semantic data models, and data visualizations. Power BI supports connectivity with numerous data sources, offering tools to integrate, transform, and prepare data for analysis. Users can then design and distribute customized reports and dashboards to facilitate data-driven decision making across teams [19].

To effectively identify and visualize critical vulnerabilities present in the system under review, Power BI Desktop was utilized in conjunction with the Tenable Nessus vulnerability scanner. The process involved running scans using Nessus to detect vulnerabilities across multiple IoT devices, exporting the scan results, and then importing this data into Power BI for analysis.

Power BI enables efficient vulnerability analysis by transforming Excel-based scan data into interactive reports and dashboards that clearly highlight affected systems. The platform's analytical capabilities allow organizations to systematically identify vulnerable software components through comprehensive sorting of scan results by severity levels and plugin identifiers. By organizing entries in chronological sequence, security teams can effectively track remediation progress and visualize their organizational risk exposure. These data-driven insights empower IT leadership to strategically coordinate patch deployment schedules and collaborate with cybersecurity personnel on targeted risk reduction initiatives.

Organizations are continually faced with various uncertainties that can impact their overall performance and longevity. Understanding how to identify and prioritize vulnerabilities for further mitigation is vital. By utilizing Power BI, organisations can consolidate data from multiple sources, multiple scanners, to get a comprehensive view of the risks facing the organisation. Leveraging Power BI's dashboard capabilities enables security teams to track critical KPIs such as exploitability that would help to validate risk mitigation effectiveness, particularly for vulnerable IoT devices like Axis cameras.

By monitoring metrics such as mean-time-to-patch (MTTP) for firmware vulnerabilities, for example CVE-2021-31986 or exploit attempt frequency on exposed RTSP ports, organizations gain actionable insights into their security posture. These visualizations allow for strategy adjustments - in case the amount of critical and exploitable vulnerabilities within IoT devices increase, teams can immediately prioritize VLAN segmentation or other remediation efforts such as for example ACAP plugin updates [81].

The Nessus vulnerability scanner's "exploit_available" plugin attribute serves as a critical indicator for identifying software vulnerabilities with known, active exploits in circulation. Security teams can analyze this data by sorting vulnerabilities based on prevalence across affected hosts. Although some plugins may appear multiple times on individual systems, most typically occur only once per host.

Vulnerabilities marked with this flag represent particularly high-risk exposures, as they enable both sophisticated attack frameworks and automated exploitation attempts by less-skilled threat actors. Organizations should treat these exploitable vulnerabilities as top-priority remediation items, requiring either immediate software updates to supported versions or complete removal of the vulnerable components.

The Power BI Desktop application was utilized to analyze and present vulnerability data, including both quantity and criticality levels, based on Tenable plugins identified for Axis, Hikvision, and Mobotix IoT devices. To enhance clarity and facilitate rapid risk assessment, a

color-coded visualization was implemented to distinguish between vulnerability severity levels and highlight vendor-specific trends. IoT devices from Axis, Hikvision, and Mobotix were assigned distinct colors, allowing for immediate visual differentiation of security issues across manufacturers.

The severity of vulnerabilities was represented using the following color scheme:

- Blue: Informational vulnerabilities
- Light Blue: Low-severity vulnerabilities
- Yellow: Medium-severity vulnerabilities
- Orange: High-severity vulnerabilities
- Red: Critical vulnerabilities

During the scan Plugin ID 105159 which is considered to be highly exploitable and is typically referred to a vulnerability in Microsoft Windows related to SMBv1 or EternalBlue-type issues was detected in Axis surveillance camera. It relates to SMB vulnerabilities such as CVE-2017-0144 which was used in major attacks such as WannaCry [76] and NotPetya. These allow unauthenticated remote code execution (RCE) over the network with no login needed. This vulnerability is wormable; it can spread across organisational networks automatically. As it is publicly exploitable such solutions as Metasploit, EternalBlue and others can exploit it in seconds therefore it should be prioritized for remediation. As recommended by Tenable to remediate this vulnerability, the latest Windows security updates should be installed. Another way to prevent attacks from taking place would be disabling SMBv1 or hardening network segmentation to block unnecessary SMB traffic. In Table 1. Plugin ID 105159 marked as red which indicates that this vulnerability is critical and requires prioritisation [83].

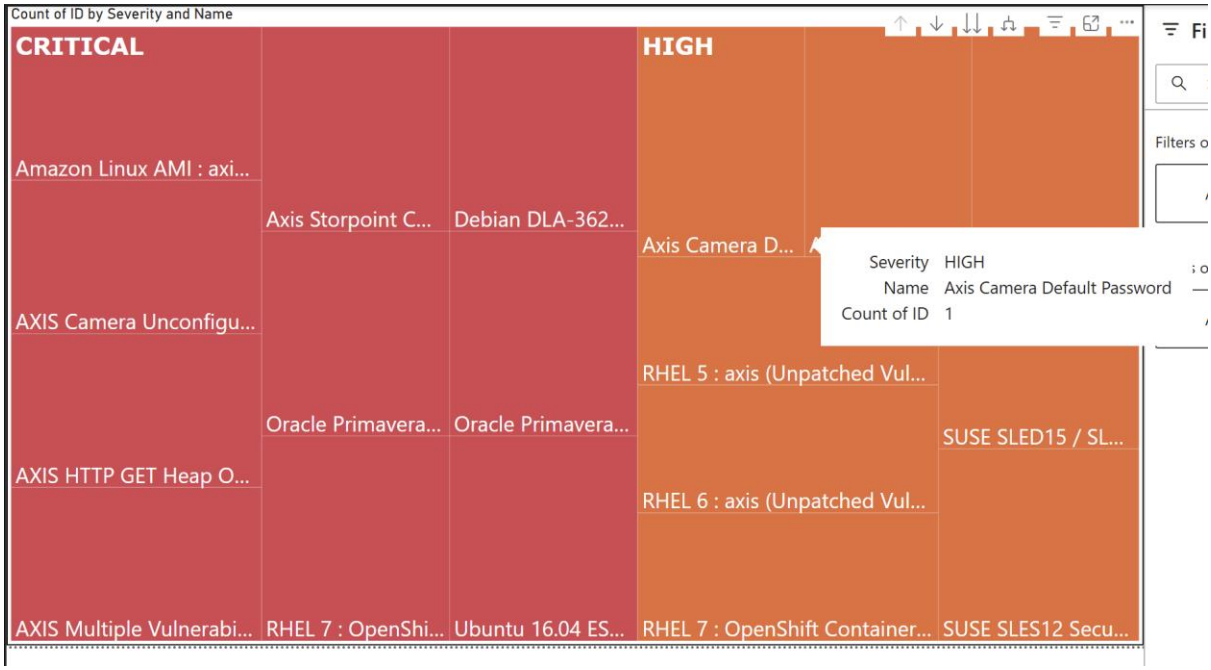

Figure 3. Axis Critical and High vulnerabilities

Another example is plugin ID 170037 detected, Table 2, Hikvision IP Camera Command Injection Vulnerability which is exploitable over the network, NAT or Internet facing devices if the web server ports 80/443 are exposed. This vulnerability poses a critical risk. It is CVSS 3.1 with the score 9.8 marked as Critical [83]. This structured visual approach enables security teams to efficiently evaluate the risk landscape of IoT deployments and prioritize remediation efforts based on severity and vendor exposure.

Figure 4. Total amount of vulnerabilities present in Hikvision

Effective dynamic risk ranking relies on three fundamental components working in concert. The Common Vulnerability Scoring System (CVSS) serves as the foundational element, offering a standardized approach to assess vulnerability severity through quantifiable metrics. By evaluating critical factors such as exploit potential and potential damage, CVSS generates numerical scores that enable organizations to objectively prioritize remediation activities.

Complementing this, exploitability metrics integrate real-world threat intelligence to gauge the likelihood of active exploitation. These metrics consider practical concerns including the existence of publicly available exploits, the technical complexity required for successful attacks, and the privilege levels needed for execution.

The framework is completed by business impact analysis, which contextualizes technical vulnerabilities within organizational priorities. This critical layer evaluates the operational

importance of affected systems, potential disruptions to business functions, data sensitivity implications, and the broader financial or reputational consequences of potential breaches.

Together, these components enable security teams to transition from static vulnerability scoring to dynamic risk assessment that balances technical severity, real-world exploit potential, and business-critical considerations.

Power BI can significantly enhance vulnerability remediation efforts by providing dynamic dashboards that prioritize risks based on CVSS scores, exploitability, and business impact. PowerBI can be connected to vulnerability scanning solutions, such as Nessus scanner, to import CVSS scores, exploitability data, and asset information to create an effective Power BI dashboard for vulnerability remediation. Design visuals help to display vulnerabilities ranked by risk level, highlighting those that require immediate attention. Setting up alerts to notify stakeholders when high-risk vulnerabilities are identified or when remediation deadlines are approaching can significantly optimize vulnerability remediation efforts.

In a financial institution, such as a bank, this type of data would be particularly valuable to several stakeholders such as Security Operations Center (SOC) Analysts or a Vulnerability Management team as they could use the visualized data to identify and prioritize critical vulnerabilities that require immediate attention. As normally IT teams are overloaded then for such teams as IT Administrators and Engineers the insights help focus remediation efforts on the most vulnerable systems, optimizing resource allocation. Risk Management Teams could better understand the potential business impact of vulnerabilities and use this data to enhance overall risk assessment and reporting to executive leadership. For CISOs and Security Executives visualization aids in communicating security risks to non-technical stakeholders, enabling informed decision-making at the executive level .

It is important to note that addressing vulnerabilities within a single IoT system, such as fixing a specific device from one vendor, will never be sufficient to secure the overall environment therefore there is the need for a holistic approach. IoT systems operate as interconnected ecosystems, and vulnerabilities in one device can be leveraged to compromise others within the same network. For example, a vulnerability in a low-priority surveillance camera could be exploited as an entry point for lateral movement, potentially leading to the compromise of critical assets such as servers or databases [82].

Data visualization transforms raw information into meaningful visual representations that enhance comprehension and highlight key insights. By presenting data in intuitive graphical formats, complex patterns and relationships become immediately apparent, enabling faster analysis and more effective communication of findings. While Power BI excels as a

comprehensive business intelligence platform for creating interactive reports and dashboards, Neo4J specializes in managing and revealing intricate connections within interconnected datasets [34].

These visualization tools significantly reduce the manual effort required for data analysis. For IoT-generated data in particular, effective visualization enables rapid pattern recognition that is critical for deriving actionable insights and informing strategic decisions. The process serves dual purposes - it simultaneously presents analytical findings while preserving the context of the original data.

Beyond simple presentation, data visualization performs deeper analytical functions. It reveals hidden correlations, emerging trends, and subtle patterns that might otherwise remain obscured in tabular data. By aligning these discoveries with organizational objectives, visualization bridges the gap between raw data and strategic decision-making. It transforms abstract numbers into compelling data narratives that stakeholders at all levels can understand and act upon [87].

4. Security Risk Management and Assessment in Internet of Things

Risk management constitutes a systematic approach to identifying potential threats to organizational assets, assessing these risks in relation to asset criticality and mitigation costs, and deploying appropriate safeguards to reduce exposure. This comprehensive process directly informs the development of security strategies aligned with organizational objectives [7]. Potential harm may originate from exploited vulnerabilities within information systems, security protocols, control mechanisms, or their implementation – all of which threat actors may target [8].

The evolving nature of threats necessitates continuous security enhancements, as vulnerabilities may be leveraged by any potential danger capable of breaching defenses [11]. In IoT ecosystems, cyber threats pose particularly severe consequences, capable of compromising critical infrastructure, disrupting operations, endangering public safety, or inflicting substantial economic losses on stakeholders [9][10]. In information security, risk represents the potential for adverse consequences when threats exploit system vulnerabilities, classically expressed as Risk = Threat × Vulnerability × Impact.

The foundation of any effective cybersecurity risk management process lies in first understanding the broader business context in which these risks will be addressed, rather than obstructing organizational objectives, cybersecurity risk management should actively support and enable them. By clarifying the operational and strategic context including the organization's core functions, priorities, and potential vulnerabilities leaders can gain critical insights into what truly matters to the business. This foundational understanding must precede the identification and mitigation of specific cybersecurity risks, ensuring alignment with the organization's mission and values [56].

Threat Analysis should assess potential threats to each asset, using data collected from IoT devices as well as likelihood or estimation of the probability evaluation of threat occurrences, using deterministic or stochastic models that account for asset vulnerabilities and attacker behavior. Then impact assessment should be performed to determine the severity of potential loss events. High-impact scenarios that could cause catastrophic damage should be prioritized for mitigation. And as a final phase a risk scoring to quantify risks by combining probability estimates and impact assessments to generate risk scores, guiding decision making on security measures [63].

Asset security frameworks establish critical organizational resources requiring protection and define the security standards necessary to safeguard them. Within this paradigm, an asset constitutes any entity of value that contributes to organizational objectives, broadly categorized as either business assets or organizational assets. Business assets represent the intangible elements fundamental to operations - including proprietary information, operational processes, organizational capabilities, and specialized competencies.

Security criteria (alternatively termed security properties) articulate protection requirements through defined constraints on business assets. These criteria form the foundation for establishing security objectives, traditionally expressed through the core principles of confidentiality, integrity, and availability:

- Confidentiality ensures business assets remain protected from unauthorized access or disclosure, maintaining appropriate information access controls while safeguarding privacy and proprietary data [90]. This principle enforces strict regulation of information dissemination to approved entities and processes.
- Availability guarantees authorized users reliable, on-demand access to critical business assets. The principle mandates systems maintain consistent operational capacity to deliver information when required, preventing disruptive denial of service scenarios.
- Integrity protects business assets from unauthorized alteration or corruption, preserving both accuracy and completeness. Accuracy safeguards prevent improper data modification, while completeness controls defend against malicious deletion or tampering. Collectively, integrity mechanisms ensure information authenticity while providing non-repudiation capabilities.

This tripartite security model establishes comprehensive protection for business-critical assets against modern threat landscapes while supporting organizational mission requirements.

The flowchart below illustrates how ISO 27001 principles apply to supplier risk management in IoT environments. It maps the relationship between organisational assets both business and system, the CIA Triad (Confidentiality, Integrity and Availability), and their role in securing IoT systems. It shows how core security criteria align with potential threats and protection measures across the IoT assets lifecycle, culminating in secure information processing in IoT systems.

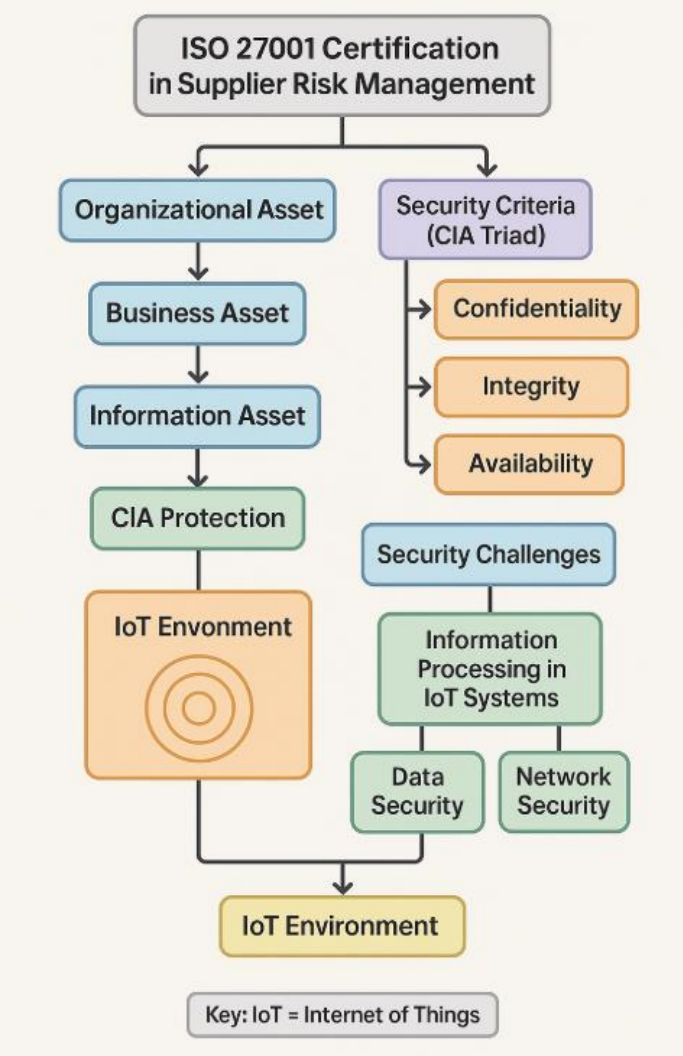

Figure 5. ISO 27001 Framework for IoT Security and Supply Risk Management

Regardless of size, every organization with IoT deployments should have cybersecurity policies in place to protect its assets [64]. The size of an organization does play a role in determining the scope, complexity, and type of cybersecurity documentation needed, but even small IoT implementations face significant risks. It is recommended to define the scope for IoT Risk assessment which requires special considerations of all connected devices and their communication protocols, cloud interfaces and mobile app connections, third-party vendor components in the IoT supply chain, physical access points to IoT devices. A standard security risk assessment typically would include:

Identifying the assets that are most valuable to the company. In the case of IoT security risk assessment. In IoT security, these include connected devices and related services.

The ISO/IEC 27001 standard, jointly developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), establishes internationally recognized requirements for implementing and maintaining an effective Information Security Management System (ISMS) within organizations. As a comprehensive framework, it mandates the integration of information security into an organization's core business processes, management systems, and the design of information systems and controls. Applicable to organizations of all types, sizes and sectors, ISO/IEC 27001 represents a certifiable standard that has demonstrated consistent global adoption growth [93]. The standard emphasizes the importance of continual improvement in information security practices, ensuring they remain effective and aligned with evolving organizational needs and threat landscapes [93].

The application of ISO 27001 in managing supplier risks within IoT systems. It categorizes organizational assets into business and system types, aligns them with the CIA Triad security criteria, and maps these to specific IoT implementation challenges. The ISO 27001 Framework for IoT Security and Supply Risk Management flowchart details how threats and protection measures are distributed across the IoT asset lifecycle and highlights the role of secure data flow from capture to display in ensuring compliance and system resilience.

It also depicts how ISO 27001 helps protect connected devices and data in IoT systems. It breaks down the different types of assets businesses use, the main security goals (confidentiality, integrity, availability), and how to keep devices and information safe at each stage of use. It connects big-picture security ideas to real-world IoT risks and protections.The evolution of standards like ISO/IEC 27001 highlights the shift toward adaptive ISMS frameworks, yet IoT demands further specialization to address its unique attack surfaces. The evolution of IoT from confined test environments to large-scale enterprise implementations has significantly expanded the attack surface, necessitating rigorous cybersecurity measures as a fundamental requirement. This transition demands systematic approaches to address the complex security challenges inherent in production IoT ecosystems. Security, privacy, and data protection are non-negotiable in deploying ethical and trustworthy IoT applications that safeguard citizens' rights. IoT systems have an expansive attack surface, involving diverse stakeholders, interconnected physical and virtual environments, and devices of varying sizes and complexities. In such a multi actor setting, cyber risks are perceived differently by different

parties, making a one-size-fits-all solution unfeasible. The current regulatory landscape for IoT safety and liability remains fragmented across EU and national jurisdictions, creating significant implementation challenges. However, emerging digital technologies present viable solutions through advanced testing and validation capabilities that can strengthen cybersecurity in complex IoT deployments [63].

To support the secure integration of IoT systems within industrial environments, the Reference Architectural Model for Industry 4.0 (RAMI 4.0) provides a structured and standardised framework. RAMI 4.0 is a three-dimensional reference architecture developed to describe all essential aspects of Industry 4.0 systems, combining elements of IT, industrial automation, and business processes. It helps organisations systematically map physical and digital assets, their functions, lifecycles, and communication layers. The importance of RAMI 4.0 lies in its ability to align technical components with business objectives, ensuring that all assets including those in IoT ecosystems are consistently categorized and understood in terms of their role, context, and interdependencies.

Traditional risk assessment methods work for small systems but fail for IoT's connected complexity where one weak device can endanger an entire network. The growing complexity of IoT technologies and ecosystems challenges traditional risk assessment methods and regulatory approaches. IoT environments in general, demand specialized assessment methodologies that extend beyond conventional IT practices. This is where graph based models play a significant role.
This structured mapping is essential for effective threat and vulnerability risk modeling, as it allows security analysts to:

- Identify and classify assets across all layers of the architecture, for example, physical devices, data, business processes.
- Understand how assets interact throughout their lifecycle, for example, development, operation, maintenance, decommissioning, which is critical for assessing lifecycle-specific vulnerabilities.
- Evaluate threats and attack vectors in context — for example, distinguishing between threats at the integration layer, for example, protocol-level attacks, versus the business layer such as process manipulation or fraud.

When combined with security criteria such as confidentiality, integrity, and availability, RAMI 4.0 enables a comprehensive and layered approach to security. It ensures that risks are not analyzed in isolation, but within the broader scope of industrial processes and IoT infrastructures. Moreover, it supports interoperability and standardization, which are essential in complex environments where assets from different vendors and technologies must operate securely and reliably together [91].

The first step in any threat modelling or assessment process is to understand who might pose a threat to you, your organisation, the system or service you are building or the information it stores and processes. For example, some organisations may be attractive targets for cyber criminals because of what they do, some may be targeted by disgruntled employees (insiders), whereas others may be attractive targets for hostile state actors because they contribute to the defence and government [56]. By using such frameworks as MITRE ATT&CK or RAMI 4.0 in conjunction with threat and vulnerability modeling techniques, organisations can better visualise their digital landscape, prioritize high-value or high-risk assets, and develop context-aware security controls. This integrated approach enhances the ability to design secure-by-design industrial systems, anticipate emerging threats, and maintain resilient operations in Industry 4.0 settings.

Further in the research it will be explored how graph modeling, combined with adversarial frameworks like MITRE ATT&CK enhances IoT risk assessment by enabling dynamic threat prioritization, and mitigation strategies aligned with organizational missions. Case study, including Axis camera deployments and VLAN-hopping scenarios, will illustrate its practical application in mitigating IoT's "connected complexity."

By integrating frameworks like MITRE ATT&CK, graph models contextualize adversarial behaviors as an example, T1190 Exploit Public-Facing Application within IoT-specific attack paths, transforming abstract risk equations (Risk = Threat × Vulnerability × Impact) into actionable insights. This approach addresses critical gaps identified in conventional methodologies, such as an interdependency analysis within which it will be Identified how a single vulnerable device such as an unpatched Axis camera jeopardizes the entire network. Graph databases like Neo4j enable organizations to map nodes such as devices, users, vulnerabilities and edges such as communication paths, exploit chains, revealing hidden risks such as lateral movement via compromised cameras or third-party firmware weaknesses.

Practical applications of this approach will also be researched, including case studies demonstrating how graph modeling enhances threat detection, risk quantification, and mitigation planning for IoT environments.

4.1 Overview and Limitations of Threat Assessment Models

Traditional risk assessment methods rely on periodic reviews, which can leave organizations exposed to emerging threats between evaluations. These gaps occur when systems evolve, new vulnerabilities are discovered, or previously underestimated risks materialize. While this limitation affects all technologies, it is particularly problematic for IoT environments due to their dynamic nature. IoT systems constantly change as new devices connect, configurations shift, and unexpected interactions arise. Conventional approaches struggle to account for these rapid developments, often failing to anticipate risks from devices that may join the network in the future.

Traditional methods help manage security challenges, and organizations have long relied on risk prioritization frameworks such as STRIDE, DREAD, and PASTA. These models will be briefly reviewed in the upcoming chapter of this research to understand their structure and application. However, while these frameworks offer foundational insights, they are not ideally suited for the unique complexities of IoT environments. The diversity of device types, scalability demands, and constantly evolving attack surfaces in IoT systems require more dynamic and adaptive risk assessment strategies. Traditional models may fall short in capturing IoT's real-time threats and unpredictability. As a result, modern security practices must emphasize continuous monitoring, automated threat detection, and proactive risk modeling to remain effective. Without these advancements, organizations risk leaving critical vulnerabilities unaddressed in an increasingly connected world. Prioritisation and response can be achieved with a wide range of techniques. Most well known frameworks are STRIDE which is simple and suitable for small organizations, DREAD is quantitative and for mature security practices and PASTA which is comprehensive and ideal for large organizations. Each framework has its strengths and weaknesses, and the choice depends on the organization's specific needs and circumstances [86].

The distinctive security challenges inherent to IoT systems including resource limitations, heterogeneous protocols, and massive deployment scales necessitate critical evaluation of whether conventional risk models can adequately address these vulnerabilities. A thorough

examination of existing frameworks' capabilities, constraints, and flexibility reveals whether they offer sufficient protection for IoT ecosystems or if novel methodologies are required to counter evolving threats.

Traditional periodic risk assessments, typically initiated by organizational changes, process modifications, or emerging threat intelligence, suffer from inherent gaps that are particularly acute in IoT environments. These evaluations may fail to identify developing risks or be delayed until after threats materialize a systemic weakness [6] that becomes critically amplified by IoT's dynamic nature. The rapid scalability of IoT implementations creates high probabilities of new system components emerging between assessment cycles, demanding predictive capabilities that current methodologies lack. Effective IoT risk management would require anticipatory assessment of potential future system configurations prior to their deployment [6]. Thus, IoT risk assessments should evaluate both active devices and potential future connections

4.2 DREAD – Security Risk Assessment Model

Threats are categorized based on severity levels ranging from critical to low, with each tier reflecting distinct mitigation priorities. High-risk threats demand immediate remediation due to their substantial potential to compromise systems or software functionality, requiring prompt implementation of protective measures. While medium-risk threats still necessitate resolution, they permit a more measured response timeline compared to their high-risk counterparts. Low-severity threats may be intentionally deferred, as their limited impact justifies lower urgency in mitigation efforts. For systematic risk evaluation, the DREAD assessment model provides a structured framework, analyzing factors such as potential damage, attack reproducibility, exploit feasibility, affected user scope, and vulnerability discoverability to generate comprehensive risk profiles.
Following the rating of the risks, a risk score is determined using the formula Risk Score = (Damage + Reproducibility + Exploitability + Affected users + Discoverability)/5 [85].

Having identified critical vulnerabilities in the target CCTV camera systems, the DREAD model will now be applied to systematically evaluate and prioritize associate threats based on their potential impact and risk level. Each criterion is rated on a scale from 0 to 10. The overall risk score is calculated as the sum of the scores across all five categories. The detailed approach is described below:

1. Assigning scores (0–10) for each DREAD category for each vulnerability.
2. Computing the overall DREAD score for each vulnerability (e.g., sum or average).
3. Using the DREAD scores to classify vulnerabilities into risk levels:

    - Low: 0–2
    - Medium: 3–5
    - High: 6–8
    - Critical: 9–10

Example for such vulnerability as Hikvision IP Cameras Improper Authentication (CVE-2013-4976)

- Damage Potential: 9 (Critical access if exploited).
- Reproducibility: 8 (Exploitation is relatively easy to reproduce).
- Exploitability: 10 (No authentication needed; easily exploitable)
- Affected Users: 9 (Affects a large number of devices globally).
- Discoverability: 10 (Known vulnerability with public exploits).

Table 2. Prioritization of CCTV Security Threats Using DREAD Scoring

ID	Name	D	R	E	A	D	Risk Level	Score
107056	Hikvision IP Camera Remote Auth Bypass	9	8	10	9	10	Critical	9,2
170037	Hikvision IP Camera Command Injection	8	7	9	8	9	High	8,2
502300	Hikvision Improper Authentication (CVE-2017-7921)	10	9	10	10	9	Critical	9,6
502305	Hikvision IP Cameras Privilege Escalation	7	6	7	7	8	High	7
502314	Hikvision Buffer Overflow (CVE-2018-6413	6	5	6	6	6	Medium	5,8
502307	Hikvision Buffer Overflow (CVE-2023-28811)	5	4	5	4	5	Medium	4,6
502311	Hikvision NULL Pointer Dereference	2	3	3	2	3	Low	2,2

4.3 Countermeasure Plan Based on DREAD Threat Assessment Model

Building a countermeasure plan for the identified vulnerabilities involves systematically addressing risks based on their severity, impact, and exploitability.

Table 3. Countermeasure Plan Framework based on NIST Risk Management Framework

RMF Step	Countermeasure	Description	Threats Mitigated	CCTV-Specific Example
Prepare	Asset Inventory & Governance	Identify all CCTV components (cameras, NVRs, storage devices) and assign security responsibilities.	Untracked devices, unclear responsibilities leading to unmanaged risks.	Maintain an up-to-date inventory of all CCTV equipment and designate a security officer responsible for system oversight.
Categorize	System Classification	Determine the impact level (Low, Moderate, High) based on the sensitivity of the areas monitored.	Misclassification leading to inadequate protection measures.	Classify cameras monitoring public areas as Low impact and those in sensitive areas (e.g., data centers) as High impact.
Select	Control Selection	Choose appropriate security controls (e.g., encryption, access controls) based on risk assessment.	Implementation of ineffective or excessive controls.	Select AES-256 encryption for video storage and role-based access controls for system users.
Implement	Control Implementation	Deploy the selected controls and document their configurations.	Misconfigurations leading to vulnerabilities.	Configure NVRs to enforce strong password policies and disable unused services.
Assess	Control Assessment	Evaluate the effectiveness of implemented controls through testing and validation.	Undetected control failures or inefficiencies.	Conduct penetration testing to assess the resilience of the CCTV network against unauthorized access attempts.
Authorize	Risk Acceptance	Obtain formal approval to operate the CCTV system after ensuring risks are at acceptable levels.	Operating without formal risk acknowledgment.	Present assessment reports to senior management for approval before system deployment.
Monitor	Continuous Monitoring	Regularly review system logs, alerts, and performance metrics to detect anomalies.	Emerging threats and system changes going unnoticed.	Implement a Security Information and Event Management (SIEM) system to monitor CCTV logs in real-time.

The table above presents a Countermeasure Plan Framework for CCTV systems based on the NIST Risk Management Framework (RMF). It outlines seven key RMF steps such as Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor and aligns each with specific countermeasures, threats mitigated, and CCTV-specific examples. These steps focus on identifying assets, classifying system impact, selecting and implementing security controls, evaluating effectiveness, gaining operational approval, and continuously monitoring for threats to ensure a secure and well-managed CCTV system.

Risk Prioritization using the DREAD matrix:

- Critical risks (scores 9–10): Address immediately.
- High risks (scores 7–8): Prioritize but address after critical risks.
- Medium risks (scores 4–6): Mitigate where feasible; implement monitoring.
- Low risks (scores 1–3): Monitor; address in the long term or as part of routine updates.

4.4 Is Dread Model Effective to Assess Risks in IoT

While the DREAD threat assessment model offers a structured and accessible framework for evaluating vulnerabilities, it falls short when applied to the complexity and scale of modern IoT ecosystems. Designed to score threats across five categories—Damage, Reproducibility, Exploitability, Affected Users, and Discoverability—the DREAD model allows analysts to derive an average risk score and classify threats into levels such as low, medium, high, or critical. For example, vulnerabilities like the Hikvision Improper Authentication (CVE-2017-7921) clearly demonstrate the model's utility in rating threats based on ease of exploitation and impact on users. However, while this method can be effective in isolated scenarios, it lacks the depth required to assess interconnected systems, which are inherent to IoT environments.

IoT devices such as CCTV cameras, smart HVAC controllers, or industrial sensors are rarely standalone. They are often embedded into broader, distributed networks, introducing interdependencies between hardware, firmware, connectivity, and software supplied by multiple third-party vendors. In such dynamic and distributed environments, DREAD's static, subjective scoring fails to account for cascading risks across supply chains or systemic vulnerabilities that manifest through multi-hop attack paths. The model assumes linear cause-and-effect relationships and treats threats as isolated incidents, which is misaligned with the

real-world behavior of IoT threats such as botnet recruitment, lateral movement across segmented networks, or coordinated distributed denial-of-service (DDoS) attacks.

Moreover, IoT devices commonly have limited computational resources and constrained environments, where routine patching, granular access control, or continuous monitoring are not always feasible. These limitations make traditional countermeasure planning, even when guided by DREAD, difficult to execute comprehensively. For instance, even if a camera vulnerability receives a “critical” score under DREAD, remediation might be delayed due to firmware update limitations, lack of vendor support, or operational dependencies that prevent device isolation.

The manual nature of DREAD scoring introduces another critical drawback its subjectivity. Without a standardized, automated baseline, the model relies heavily on individual analyst interpretation, which may vary across assessors and contexts. This inconsistency makes it unsuitable for large-scale risk assessments or for environments requiring real-time threat response. Furthermore, DREAD does not incorporate environmental or behavioral context, such as threat actor capability, exploit availability in the wild, or the systemic risk amplification that occurs when multiple devices are compromised simultaneously.

In conclusion, while DREAD offers foundational value in small-scale threat prioritization, its limitations in scalability, contextual awareness, automation, and adaptability make it ill-suited for modern IoT risk management. Instead, more context-aware models like STRIDE or graph-based frameworks using technologies such as Neo4j, which allow visualization of interdependencies and automated correlation of security data (self-assessments, CVE scan results, and device behavior), provide a more accurate, dynamic, and operationally useful approach to securing interconnected IoT ecosystems. As threats become more complex and interconnected, so too must our models of assessing and responding to them.

While the DREAD model provides a structured approach to assessing vulnerabilities, it may not be the most effective method for evaluating IoT security risks, particularly in devices like CCTV cameras. For example, the Hikvision Improper Authentication vulnerability (CVE-2017-7921) scored critically across all DREAD categories, highlighting its severity. However, DREAD does not account for the large-scale, automated exploitation of IoT devices, such as botnet attacks that could compromise thousands of vulnerable cameras simultaneously.

Additionally, IoT devices often have resource constraints, making certain mitigation measures like frequent patching or advanced monitoring—challenging to implement. The model's reliance on subjective scoring can also lead to inconsistencies, particularly when assessing the risks of interconnected devices rather than isolated vulnerabilities. Given these limitations, alternative frameworks that incorporate real-world IoT threat scenarios, such as STRIDE or AI-driven risk assessment models, may offer a more accurate and comprehensive approach to securing IoT ecosystems.

4.5 STRIDE – Threat Modeling Framework

In this section, we explore how the STRIDE threat modeling framework can be applied to a real-world use case involving an IoT device. This approach allows us to systematically identify potential security threats and better understand the limitations of traditional threat modeling when applied to modern, interconnected environments. To analyze threats using the STRIDE model for the Axis camera case study, this research employs the Microsoft Threat Modeling Tool (2016) [95]. Microsoft's STRIDE framework provides a systematic approach to security threat identification by categorizing risks into six distinct threat types. The model encompasses Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege threats, each corresponding to fundamental security principles. These threat categories directly align with core security properties: Spoofing relates to authentication vulnerabilities, Tampering compromises data integrity, Repudiation challenges non-repudiation controls, Information Disclosure breaches confidentiality, Denial of Service impacts system availability, and Elevation of Privilege undermines proper authorization mechanisms [94,96].

STRIDE was developed by Kohnfelder et al. in 1999 and adopted by Microsoft in 2002 [101] as part of its Secure Development Life Cycle (SDLC) [72] and Threat Modeling Tool (TMT) [74]. STRIDE focuses on identifying threats violating software security, emphasizing networked system. It covers Spoofing (lack of authentication), Tampering, Repudiation, Information disclosure, for example, data breaches, Denial of Service, and Elevation of privilege threats. A STRIDE user takes a DFD – Data Flow Diagram or other system models and for each element in the attack surface lists possible threats in each STRIDE category. The threat listing can be semi-automated using an attack library. Microsoft has documented its STRIDE threat modeling approach since 1999 and provided some useful lessons learned, such

as the lack of threat modeling training, complexity in real-world scenarios, and the importance of the people factor [101].

By applying STRIDE to an Axis security camera, both its usefulness and its limitations in the context of IoT systems will be demonstrated. A simple yet critical process user password setting and storage will be modeled and evaluated how well STRIDE captures the real-world risks associated with this functionality in an embedded, networked device. This analysis also serves as a foundation to critique STRIDE's scalability and adaptability in complex enterprise environments with heterogeneous devices and dynamic network topologies.

Figure 6. illustrates a traditional Linux-based password-setting flow where an employee sets a password. This password is processed via /bin/password, a binary with SetUID permission. As a result the password hash is stored in /etc/shadow, a protected file. In the below section we will apply the above scenario to an Axis security camera deployed in a corporate environment.

- User (Employee/Admin): Uses a web UI or command-line interface to set the admin password of the camera.
- Set Password Functionality: Internally, the Axis camera might run a lightweight Linux OS, for example, BusyBox, which invokes a SetUID binary or script (similar to /bin/password) to handle password changes.
- Password Storage: The password hash is stored in a configuration or credentials file (not always /etc/shadow, but something functionally similar) on the camera's internal storage.
- SetUID Context: The SetUID behavior is essential because the script or binary might need root privileges to access or modify sensitive files.

STRIDE is useful for basic threat modeling, but it has several limitations when applied to IoT environments like Axis cameras or large enterprise networks. In enterprise settings, where thousands of interconnected devices such as cameras, sensors, and firewalls coexist, STRIDE's manual and asset-specific approach becomes unmanageable. The framework relies on static diagrams, which struggle to reflect the dynamic nature of IoT systems that frequently undergo firmware updates, network changes, and configuration shifts.

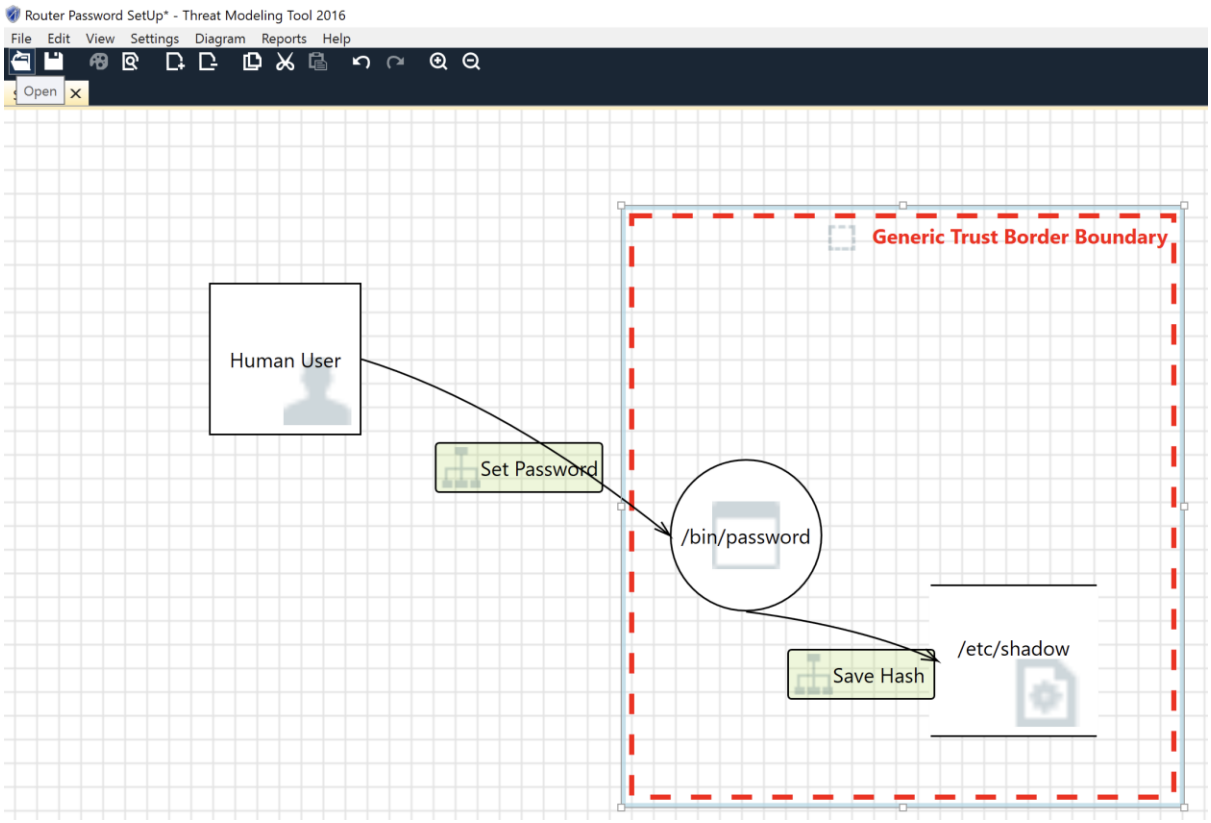

Figure 6. STRIDE model for the Axis camera case study employing the Microsoft Threat Modeling Tool (2016).

Furthermore, STRIDE is too generic to address the unique constraints of embedded devices, such as limited memory or the absence of trusted platform modules. For example, in the case of Axis cameras, it would fail to capture important risks like the absence of secure boot mechanisms, unencrypted firmware, or vulnerabilities in RTSP streaming. Another critical drawback is that STRIDE identifies threat categories but does not assess their severity or likelihood, making it less effective for prioritizing risks in complex environments. As a result, other models such as DREAD, PASTA, or attack trees are often more appropriate for enterprise IoT.

There's also the danger that STRIDE can lead to a false sense of security. Teams might consider the threat modeling process complete after producing a STRIDE diagram, even though they may have only addressed a small subset of the actual risks. To overcome this, STRIDE should be used alongside techniques like asset classification, network segmentation analysis, and automated threat intelligence. Frameworks such as MITRE ATT&CK for ICS/IoT and PASTA offer a more comprehensive view of threats [96].

In the specific case of modeling a password-setting process on an Axis camera, STRIDE might successfully identify localized risks. However, it lacks the scalability and flexibility needed to capture the full threat landscape in dynamic, interconnected IoT environments. It is best regarded as an initial step rather than a complete solution.

5. Introduction to Graph Theory in Cyber Security Through Neo4J

Neo4j is a graph database that stores data in a graph. Data is stored as nodes and relationships instead of tables or documents. Graph databases are particularly useful when the connections between data are as important as the data itself. The objects are referred to as nodes (vertices) connected by relationships (edges). Neo4j uses the graph structure to store data and is known as a labeled property graph. Storing data in rows and columns is one of the oldest storage mechanisms and existed long before the computer. Tabular data is a tried-and-tested methodology that works well for many use cases. However, as the amount of data grows or the application or use case becomes more complex, challenges dealing with relationships might occur. Data within Neo4j is stored and organized using nodes, relationships, labels and properties [121].

- Nodes are the circles in a graph. Nodes typically represent objects or entities.
- Relationships are the lines in the graph. Relationships describe how nodes within the graph are connected to each other.
- Labels Nodes are grouped by or categorized using labels. Labels describe what the nodes are, for example, Router, Switch, Host etc.,
- Properties are named key, value pairs

Relationships in a graph are treated with the same importance as nodes that connect them.
When we create a relationship between two nodes, the database stores a pointer to the relationship with each node. When reading data, the database will follow pointers in memory rather than relying on an underlying index. This means that the query time remains constant to the size of the relationships expanded regardless of the overall size of the data. A graph database yields much faster results for queries across entities and is a great fit for this research as we need to understand the relationships between entities - for example, how two routers are connected.

Neo4J integration with such solutions as Nessus scanner from Tenable or Power BI Desktop can help to analyze security related data enabling organisations to uncover relationships and patterns for a more effective threat detection and response [122].

Tenable scanning solutions primarily output vulnerability scan results in JSON, CSV, or XML formats and to extract that data Neo4J can be integrated with Tenable.io or Nessus API to pull scan data for analysis [53]. To address fixing vulnerabilities on servers and prioritize them, the data will be modelled in Neo4j to represent servers, vulnerabilities, and their relationships. Below a simple data model example:

(:Server)-[:HAS_VULNERABILITY]->(:Vulnerability)

To prioritize vulnerabilities, we can assign severity levels to vulnerabilities and use cypher queries to depict servers with the same vulnerability. Here's an example query to find all servers with a specific vulnerability:

MATCH(s:Server)-[:HAS_VULNERABILITY]->(v:Vulnerability{name:
"SpecificVulnerabilityName"})RETURN s

By structuring data in Neo4j and running queries like the one above, we can effectively manage vulnerabilities on servers and prioritize them based on severity. Later in the research with the help of Neo4J the relationships between CCTV cameras, vulnerabilities, and other relevant entities will be modeled in a graph database. This will help to easily track and analyze vulnerabilities across different CCTV cameras, identify patterns, and prioritize security measures based on the severity of vulnerabilities. Cypher queries can be used to quickly identify CCTV cameras with similar vulnerabilities, understand the impact of those vulnerabilities, and take proactive actions to mitigate security risks.

5.1 Leveraging Neo4J for Vulnerability Assessment

This work presents a threat modeling approach that leverages graph-based analysis to understand how an attack on a vulnerable IoT device can propagate through the infrastructure if successfully exploited. In dynamic IoT environments, where devices and subsystems frequently join and leave the network, a single compromised device can serve as a pivot point for further exploitation. Traditional attack-graph approaches, designed for static networks, fail to account for these evolving interconnections, often resulting in rigid and outdated security assessments. By dynamically updating attack graphs to reflect real-time system changes, our

approach enables the identification of potential attack chains, showing how a single breach can escalate into a broader compromise within the IoT ecosystem.

IoT environments are inherently dynamic, with devices interconnecting autonomously and outside the direct control of system operators. Such evolving interconnections modify attack paths, necessitating a threat modeling approach that adapts to changing topologies. To illustrate this, we examine CVE-2017-0144, a heap overflow vulnerability in Axis devices that can be exploited via a malicious HTTP GET request. This use case highlights how an attacker can exploit a newly introduced device with a known vulnerability, demonstrating how changes in an IoT environment impact security risks.

To support the analysis, the proposed approach using Neo4j was implemented, a graph database management system (GDBM) well-suited for mapping, visualizing, and querying interconnected data. By dynamically updating attack graphs based on system changes, this approach enables efficient threat modeling that reflects the evolving nature of IoT environments. Our results demonstrate that the developed model effectively tracks system modifications, identifies emerging attack paths, and provides real-time security insights, making it a robust solution for IoT threat and risk analysis.

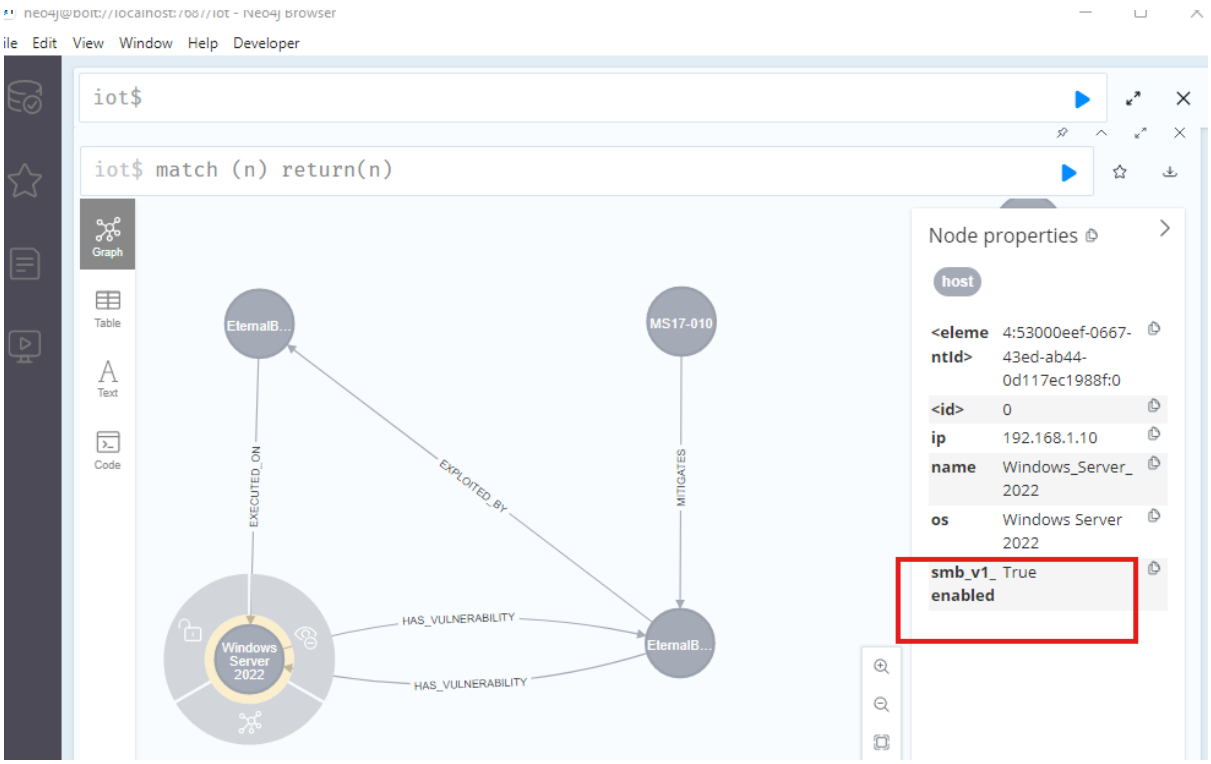

Figure 7. Relationships between systems, vulnerabilities, and potential attack paths.

The Tenable plugin database was used to explore this vulnerability. Tenable Plugin ID 105159 is associated with detecting a vulnerability in Microsoft SMBv1 due to the EternalBlue exploit (CVE-2017-0144). This vulnerability was exploited in the WannaCry ransomware attacks.

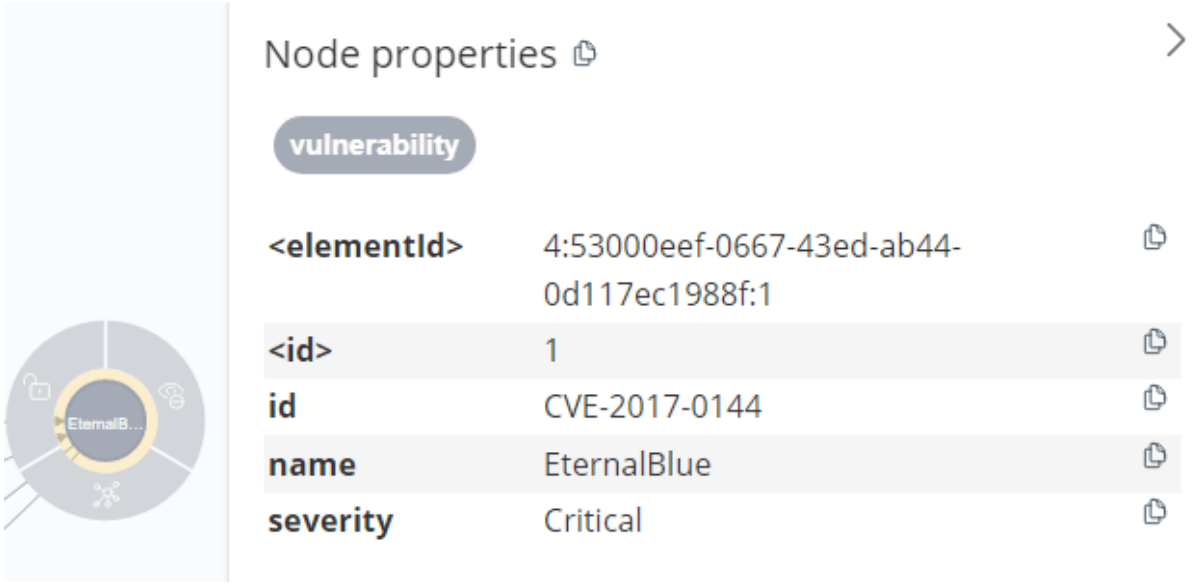

Figure 8. Critical EternalBlue vulnerability CVE-2017-0144

An in-depth explanation of how an attack using this vulnerability can potentially be executed will be provided. The SMBv1 Protocol Flaw vulnerability needs to be understood first of all. Server Message Block version 1 (SMBv1) is an outdated protocol for file sharing, printers, and communication between computers in a network. EternalBlue targets a buffer overflow vulnerability in SMBv1. By sending a specially crafted packet, an attacker can execute arbitrary code on the target system. EternalBlue Exploit is developed by the National Security Agency (NSA) and was leaked by the Shadow Brokers group in 2017. It allows attackers to gain remote code execution (RCE) on unpatched Windows systems that have SMBv1 enabled.

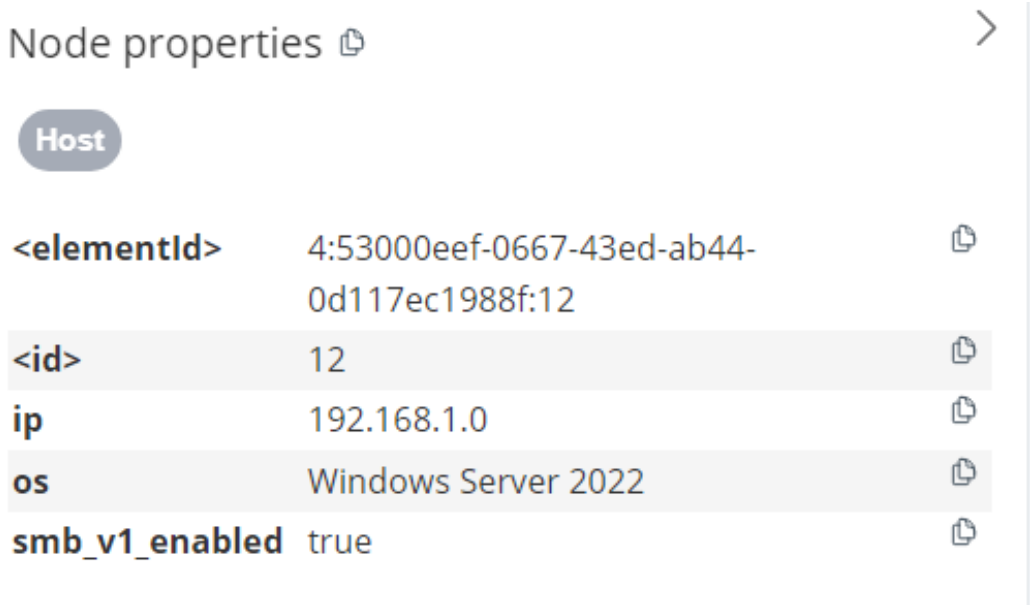

Figure 9. Detecting all Windows Server 2022 Operating System where smb_v1_enabled with Neo4J query

Network scans reveal SMBv1-enabled systems to where patch has not been yet applied.
As a first step to exploit vulnerability an attacker would need to perform a reconnaissance by scanning the network. NMAP scanner can help to identify vulnerable systems by using the following command: nmap -p 445 --script smb-vuln-ms17-010 192.168.1.0 which will scan the target system for the vulnerability detected by Tenable Plugin 105159.

In case, a vulnerability is present in the system, an attacker would need to verify if SMBv1 is enabled on the target system by using SMB scanning tools like Metasploit auxiliary modules or manual probing. Afterwards, an attacker would need to use an exploit tool such as Metasploit to leverage EternalBlue.

An attacker uses Metasploit to confirm SMBv1 is enabled and executes EternalBlue exploit:use exploit/windows/smb/ms17_010_eternalblue

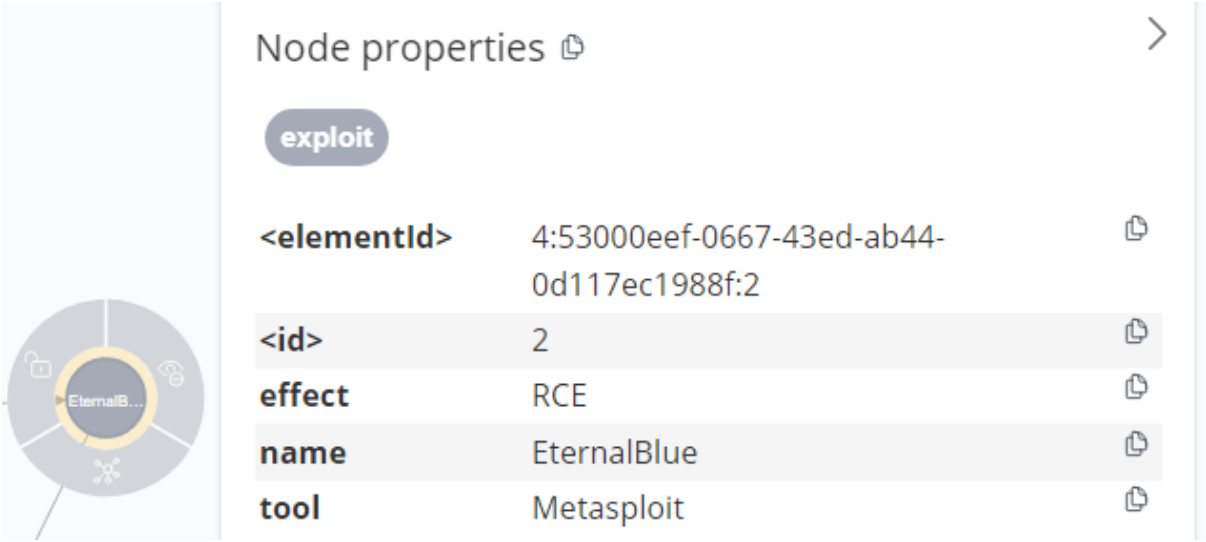

Figure 10. An attacker uses Metasploit to confirm SMBv1 is enabled to execute EternalBlue exploit

In case of a successful attack, the attacker gains control over the target system. As a follow up action, the backdoor such as DoublePulsar could be installed to successfully get back into the system at any time to proceed moving laterally within the network and as a result deploy WannaCry or perform a lateral movement to compromise a high-value crown jewel database server containing sensitive customer data.

By using Mimikatz, an attacker will be able to dump credentials from LSASS memory to obtain domain administrator credentials stored in memory, which would enable further access. Using pass-the-hash (PtH), the attacker authenticates as an admin to the database server.
Once, getting access to the server an attacker will be able to identify SQL Server, Oracle, or MongoDB instances and run SQL queries to extract customer financial data and credit card numbers. In order to extract the data an attacker can use 7-Zip or WinRAR.

To prevent the above scenario from taking place we take Tenable's recommendation to patch the servers and install Microsoft’s security update (MS17-010) to patch the SMBv1 vulnerability or disable SMBv1 on all vulnerable systems if not used.

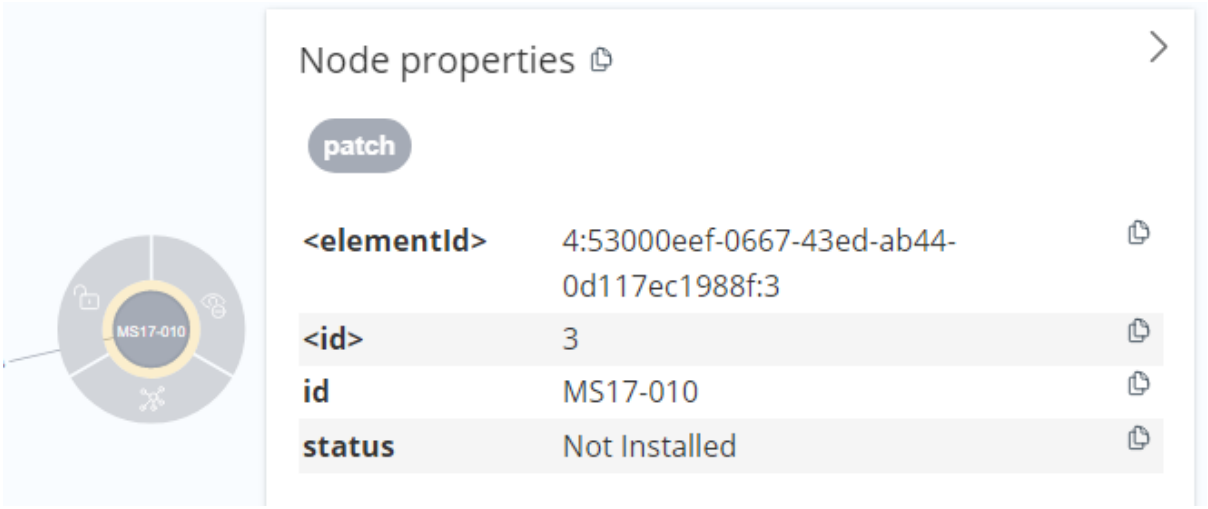

Figure 11. Patch status - Not Installed

Neo4j can be now used to detect all vulnerable hosts. A security analyst would need to use below query to visualize all vulnerable hosts.

MATCH (h:Host)-[:HAS_VULNERABILITY]->(v:Vulnerability {id: "CVE-2017-0144"})
RETURN h.ip, h.os, h.--:

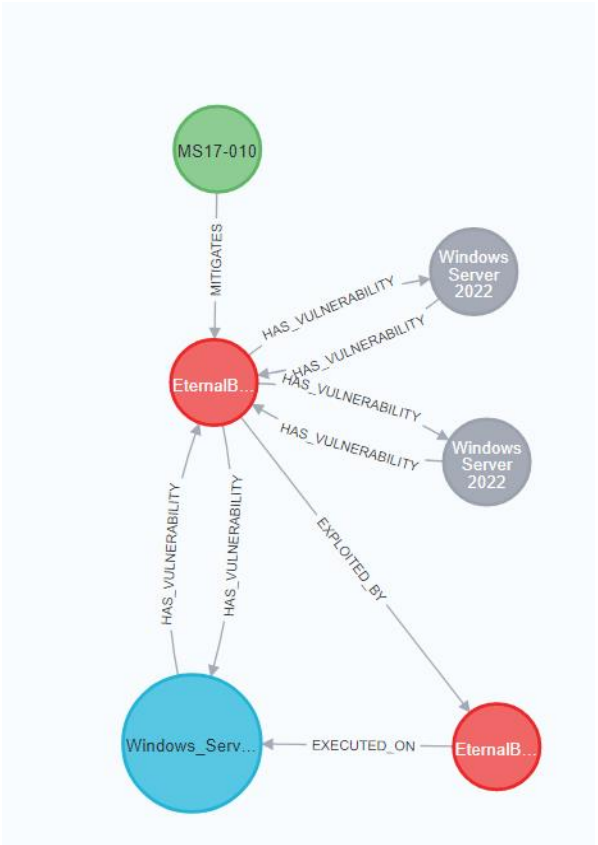

Figure 12. Detecting all Windows Server 2022 hosts with smb_v1_enabled

While patching the SMBv1 vulnerability or disabling it minimizes the risk of an attack, relying on it alone is not sufficient for robust cybersecurity. To reduce the risk of exploitation from vulnerabilities like the one identified by Tenable Plugin 105159 (EternalBlue), layered security controls must be implemented.

To complement patching Network Segmentation or dividing it into smaller, isolated segments to limit lateral movement by attacker and blocking TCP port 445, 139 where it is not needed at the network perimeter to prevent SMB traffic from entering or leaving the network. It will help the attack proliferation. If an attacker compromises one segment there will be no possibility to easily access others which would limit the spread of malware like WannaCry. Another prevention method is to implement centralized logging to detect anomalous behavior by using SIEM solutions to correlate events and detect malicious SMB traffic.

5.2 Organizational Network Topology

In the given scenario, the network infrastructure comprises routers and switches that facilitate communication between various systems, including Windows servers, Axis cameras, and database servers. The routers, 'Cisco_ENCS_5100'and 'Cisco_ISR_G1' manage traffic between different network segments, ensuring data reaches its intended destination securely and efficiently. The network infrastructure comprises multiple routers, each equipped with distinct interfaces enabling connectivity to various subnets. These routers interconnect to facilitate communication across different subnetworks. In the clinic’s network design, all routers link to a central aggregator router (Cisco_ENCS_5100, designated as Router 1), which serves as the gateway to the internet while also providing an interface to Subnet 1. Router 2 (Cisco_ISR_G1) establishes connectivity between Subnets 1, 2, and 3 while maintaining a direct connection to Router 1. Additional routers can be deployed following this same architectural pattern, with direct physical connections represented as edges between routers and end devices where applicable.

By default, all routers implement packet filtering rules that deny traffic unless explicitly permitted, enforcing strict access control. End devices within the same subnet communicate logically through their respective router rather than via direct connections, resulting in a

topology where devices connect either directly to routers/switches or to other end devices. Each connection link can be further characterized by protocol-specific attributes (e.g., TCP, UDP) to govern allowed traffic types. Switches enhance internal network efficiency by intelligently routing data packets to destination devices using MAC address resolution, ensuring optimized traffic flow.

Given the presence of vulnerabilities such as CVE-2017-0144, network segmentation and firewall rules are crucial in preventing lateral movement by potential attackers.

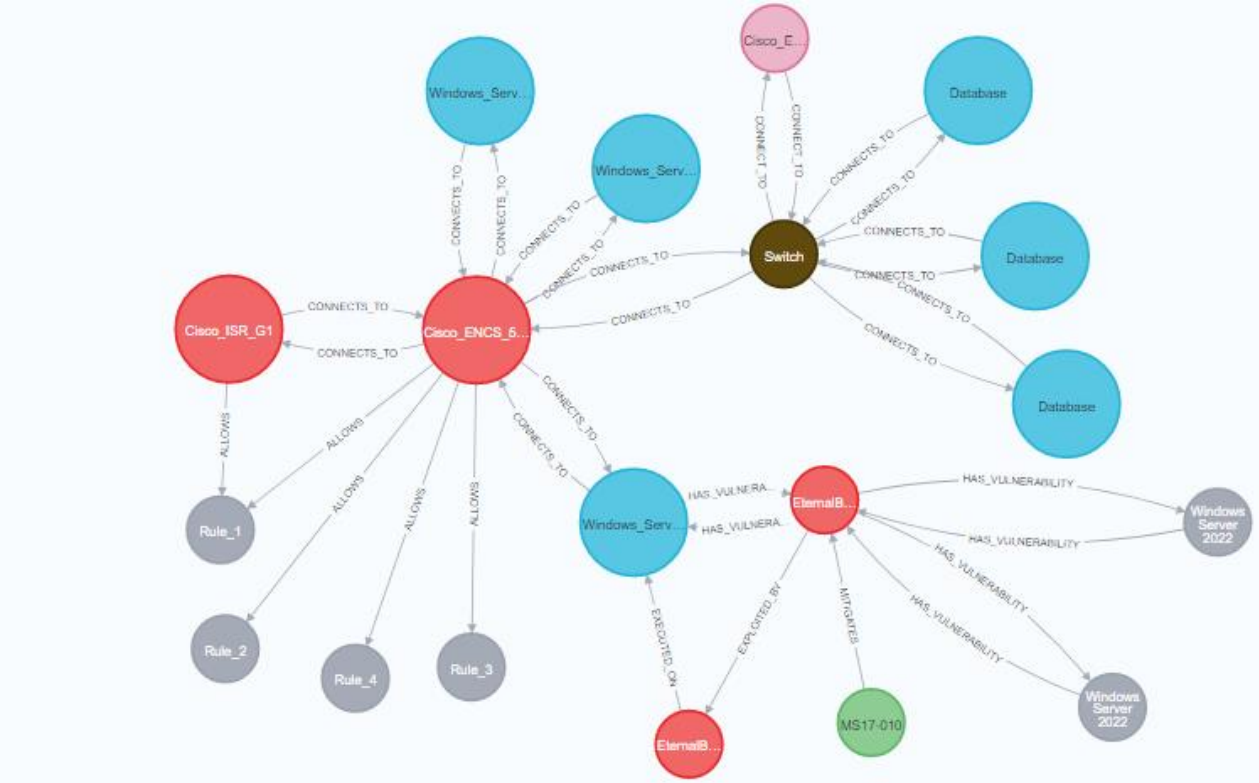

Figure 13. Organisation topology graph

Proper configuration of VLANs (Virtual Local Area Networks) and access control lists (ACLs) on switches can limit unauthorized access, while intrusion detection systems (IDS) and intrusion prevention systems (IPS) integrated into routers can help identify and mitigate exploit attempts. When utilized in this network context, we can map relationships between networking devices, showing potential attack vectors that exploit misconfigurations or vulnerabilities in the infrastructure, aiding in risk mitigation and security policy enforcement.

In this research, we demonstrated how the Neo4J graph database system plays a crucial role in assessing security risks by depicting vulnerabilities in a structured and visually intuitive manner. Using a real-world scenario while the Axis camera vulnerable to CVE-2017-0144 (AXIS HTTP GET Heap Overflow), we showed how Neo4J effectively models network topology, service dependencies, vulnerabilities, and exploitation conditions.
Through our case study, we explored an organizations' network with Windows systems, some running SMBv1, and a Windows Server 2022 environment used for centralized management server and database management. With the help of Tenable vulnerability scanner, known weaknesses were identified and mapped into the Neo4J database allowing for in-depth analysis of relationships between assets, services and potential attack vectors.

By leveraging Neo4J's capabilities, we demonstrated how security teams can:

- Visualize complex attack patch: Neo4J provides a clear representation of how vulnerabilities in different systems interconnect, aiding in understanding potential attack propagation.
- Identify high-risk areas: Through graph queries and analysis, critical vulnerabilities, such as those vulnerabilities in CVE-2017-0144, can be pinpointed based on their position in the network and the dependencies they introduce.
- Enhance risk assessment: Security teams can assess the impact of vulnerabilities by analyzing direct and indirect connections between systems, allowing for prioritized mitigation strategies.
- Support proactive security measures:
- By continuously updating the Neo4J database with new vulnerability scan and network changes, organisations can proactively identify emerging threats and reinforce defenses before exploitation occurs.

Overall, depicting vulnerabilities using Neo4J not only enhances risk assessment but also strengthens an organisation's security posture by providing a dynamic and adaptive visualization of its attack surface. This research underscores the importance of graph-based security analysis in modern cybersecurity frameworks, highlighting how graph databases can be instrumental in mitigating cyber threats effectively.

5.3 Threat Modeling for IoT Using MITRE ATT&CK Neo4J

The MITRE ATT&CK for IoT framework provides a structured way to analyze threats against IoT devices like Axis surveillance cameras. As a part of the research practical examples of how attackers might exploit these devices and how to defend against them using ATT&CK tactics and techniques in conjunction with Neo4J will be researched. As an example, an attack starts from the tactic - reconnaissance (TA0043). An attacker scans for exposed Axis cameras using Shodan, looking for open ports (HTTP/HTTPS, RTSP, ONVIF), default credentials (root:pass, admin:admin), unpatched firmware vulnerabilities using techniques such as T1595.001 (Active Scanning: IP Scanning) and T1589.002 (Gather Victim Host Information: Firmware/Software Versions). MITRE framework contains Enterprise Mitigations that represent security concepts and classes of technolog/ies that can be used to prevent a technique or sub-technique from being successfully executed. Based on mitigation actions of those techniques it is recommended to disable unnecessary services (e.g., Telnet, FTP), change default credentials and enforce strong passwords and block external access to camera admin interfaces [64,65].

As a part of Initial Access tactic (TA0001) an attack can be performed by exploiting CVE-2021-31986 (Axis Camera ARTPEC firmware flaw) to gain remote shell access, using ONVIF protocol weaknesses to bypass authentication. The MITRE ATT&CK Techniques used for this are T1190 (Exploit Public-Facing Application) and T1078.003 (Valid Accounts: Default Credentials). Based on mitigation actions for those techniques it is recommended to patch firmware regularly (Axis Security Notices), disable ONVIF if unused or restrict via firewall and use network segmentation (isolate cameras in a VLAN).

Threat modeling helps visualize attack paths, prioritize risks, and design defenses. By combining MITRE ATT&CK for IoT with Neo4j - a graph database, we will map attacker behaviors as well as identify weak points. Prior to building a graph we will need to understand components of Axis cameras using Axis documentation [57]. Based on the documentation following components need to be considered:

- Firmware (Linux-based OS)
- Web interface (HTTP/HTTPS)

- ONVIF/RTSP streaming
- Physical interfaces (USB, SD card)
- Cloud integration (AXIS Camera Station)[67]

Taking into consideration components listed above, the attack surface could be either remote via internet-facing admin panel or in case of a compromised internal network - local. As recent cases with CrowdStrike proved, a Supply chain attack is also possible via malicious firmware updates [68].

Table 4. Relevant ATT&CK for IoT techniques

Tactic	Technique (ID)	Axis Camera Example
Reconnaissance	T1595.001 (IP Scanning)	Shodan searches for exposed Axis cams
Initial Access	T1190 (Exploit Public-Facing App)	Exploit CVE-2021-31986 (firmware RCE)
Execution	T1059.004 (Unix Shell)	Malicious command via vulnerable ACAP plugin
Persistence	T1037.004 (Startup Scripts)	Modify /etc/init.d to maintain access
Lateral Movement	T1210 (Exploit Remote Services)	Pivot via RTSP to internal servers
Exfiltration	T1048.003 (Unencrypted Exfil)	Steal video via unsecured RTSP stream

As the first step we will create nodes in Neo4J:

```
CREATE (camera:AxisCamera {model: "P1448", firmware: "8.20.1"})
CREATE (attacker:Attacker {type: "APT", motivation: "Espionage"})
CREATE (vuln:CVE {id: "CVE-2021-31986", severity: "High"})
CREATE (network:Network {segment: "VLAN 20", trust_level: "Untrusted"})
```

Then define relationship:

```
MATCH (a:Attacker), (c:AxisCamera), (v:CVE), (n:Network)
CREATE (a)-[:SCANS]->(c)
CREATE (a)-[:EXPLOITS]->(v)-[:AFFECTS]->(c)
```

CREATE (c)-[:CONNECTED_TO]->(n)

In the scenario given, the main purpose of the attacker is espionage. Most cyber espionage activity is categorized as an advanced persistent threat (APT) which is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization and evade existing security measures for long periods of time [69]. In Figure 11. An author used Neo4J to depict, leveraging what type of techniques, an attacker with an espionage intent might take advantage of to perform reconnaissance in order to get an initial access to the system such as T1595.001 (IP Scanning) using Shodan or T1190 (Exploit Public-Facing App) [71].

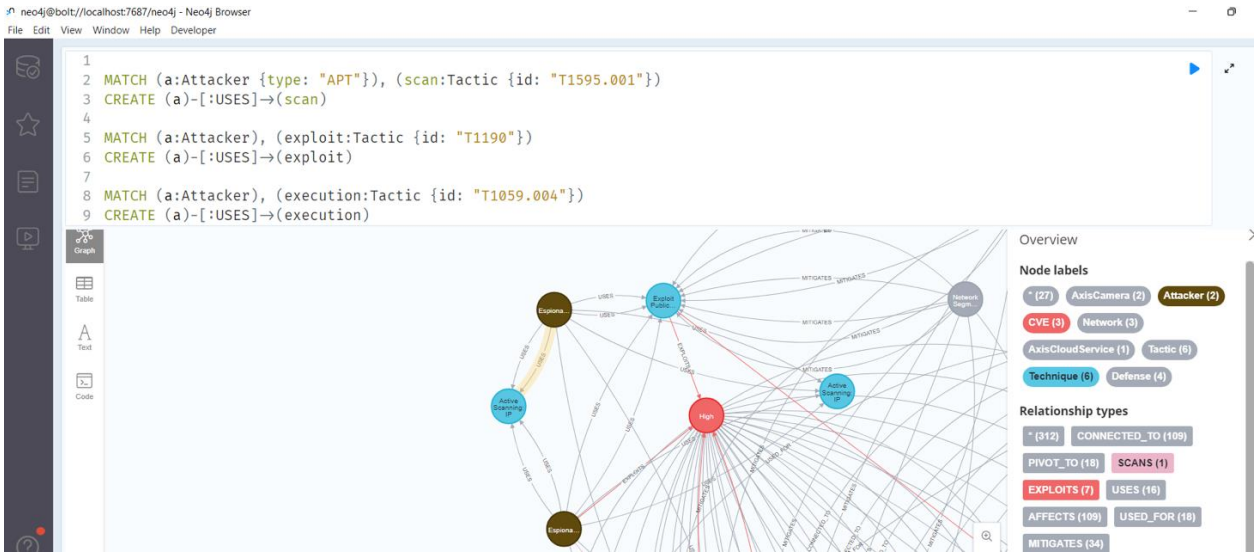

Figure 14. Visualization of T1595.001 technique used by an attacker

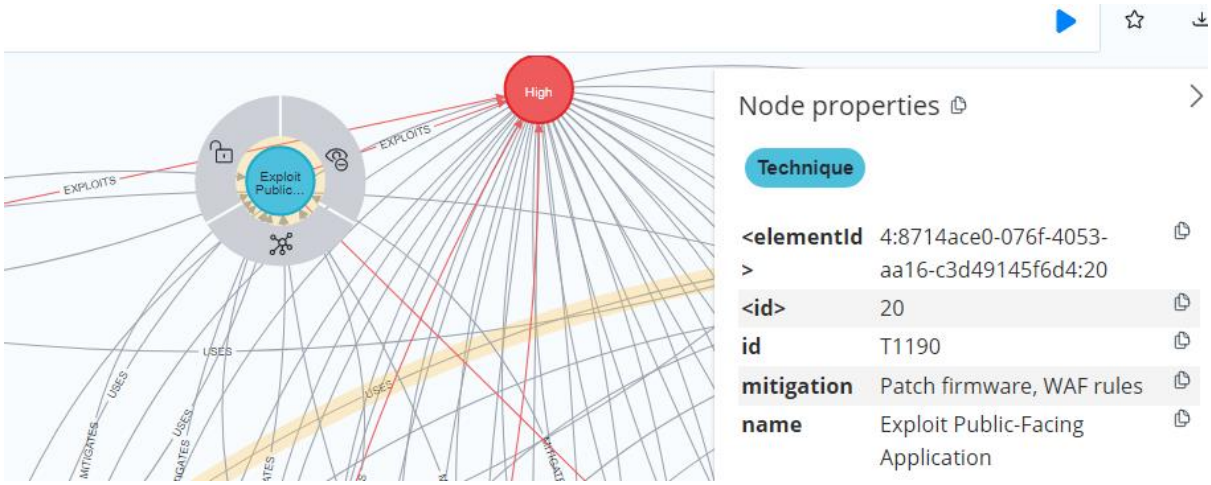

Figure 15. Visualization of T1190 technique used by an attacker with espionage intent

Cypher query language will be used to query how an attacker can move from a compromised camera to the corporate network. When initial access has been established an attacker might leverage MITRE ATT&CK technique T1059.004 (Unix Shell) to execute arbitrary commands via a Unix shell such as /bin/sh, /bin/bash on a compromised system. In the given scenario of Axis cameras with vulnerable ACAP plugins, this technique might be used for several different purposes such as gaining persistent access to the system, downloading and executing malware or pivoting to other network segments.

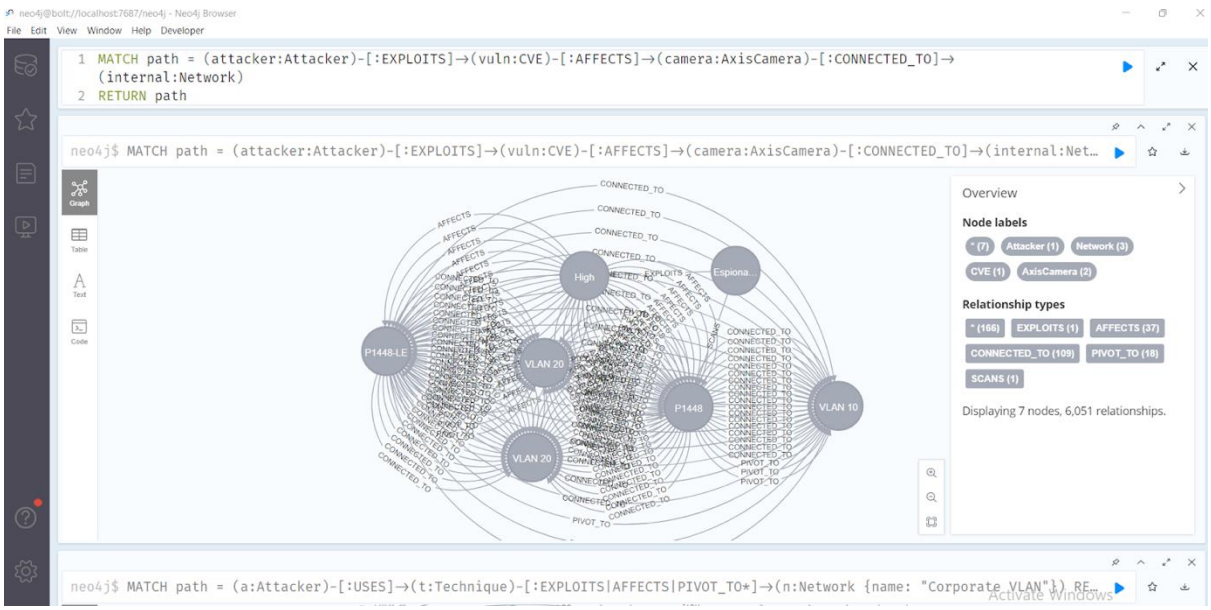

Figure 16. Visualization of the pivot attacks via RTSP/VLAN hopping

The Axis Camera Application Platform (ACAP) allows third-party applications to run on Axis cameras, but vulnerabilities in these plugins can lead to remote code execution (RCE). An attacker might exploit weak ACAP apps to execute malicious commands, hijack cameras, and pivot across networks [70]. Pivot attacks involving RTSP (Real-Time Streaming Protocol) and VLAN hopping are common in IoT environments, especially when attackers exploit misconfigured cameras and network segmentation flaws.

This paragraph explored the security posture of Axis surveillance cameras by integrating MITRE ATT&CK for IoT with Neo4j-based threat modeling, revealing critical vulnerabilities, attack pathways, and mitigation strategies. The study demonstrated that while Axis devices are widely deployed, their exposure to default credential exploits, firmware vulnerabilities and supply chain risks makes them high-value targets for attackers [58].

This analysis also demonstrates how Neo4j graph databases enhance IoT threat modeling by mapping attacker behaviors and device relationships, surpassing traditional linear methods. By integrating MITRE ATT&CK for IoT, we identify critical attack paths such as Shodan reconnaissance (T1595.001) CVE exploitation (T1190) Unix shell execution (T1059.004) lateral movement via VLAN hopping (T1574) - enabling precise risk prioritization. Neo4j visualizes cascading vulnerabilities, like how a compromised Axis camera (via ACAP plugins) exposes entire networks. Practical defenses include patching firmware, disabling unused services (RTSP/ONVIF), and network segmentation. The framework also highlights supply chain risks such as malicious firmware updates and espionage tactics such as APT persistence via startup scripts.

Combining Neo4j's relationship-based analysis with MITRE mitigations allows proactive defense. This approach is vital for securing IoT ecosystems, where interdependencies demand dynamic, graph-based threat modeling. As IoT threats evolve, combining ATT&CK's rigor with Neo4j's analytical power provides a scalable blueprint for securing not just Axis cameras, but the broader IoT ecosystem. For IoT defenders, this fusion of graph analytics and structured threat frameworks is indispensable.

6. Evaluating IoT suppliers From a TRPM or Third-Party Risk Perspective

The specialized nature of Internet of Things (IoT) technology, encompassing hardware, software, and connectivity, frequently drives organizations to outsource devices and related services. This approach reduces the burden of in-house design, development, and manufacturing. However, as IoT ecosystems become increasingly reliant on third-party vendors for critical components and infrastructure, these external partnerships introduce substantial risks if not thoroughly managed. Vulnerabilities embedded within third-party software or hardware can propagate across the ecosystem, threatening its integrity and security.

Attacks targeting one component of the supply chain often have cascading effects, impacting interconnected systems and highlighting the shortcomings of traditional, siloed security approaches. Isolated vulnerability scanning and surface-level assessments provide only partial insights, failing to account for the systemic and interdependent nature of modern IoT environments. For example, vulnerabilities in seemingly peripheral systems such as environmental controls can be leveraged to compromise mission-critical infrastructure. This was evidenced by the widely reported breach where hackers exploited internet-connected HVAC systems to infiltrate a major U.S. retail bank's network. In that case, misconfigured HVAC controllers possibly using default credentials (admin/admin) or vulnerable to CVE-2019-9566 were connected to the same VLAN as teller workstations. Attackers exploited the HVAC system's web interface, enabling lateral movement and ultimately malware deployment for ATM jackpotting attacks [112].

These incidents expose the insufficiency of fragmented security measures and underscore the importance of security frameworks that assess risks across the entire IoT supply chain. It is essential to treat vulnerabilities not as isolated findings, but as part of a broader network of interrelated risks. A graph-based approach, such as one built using Neo4j, can model these multidimensional relationships to offer the contextual understanding necessary for meaningful risk mitigation. As this research illustrates, such graph-powered frameworks allow organizations to visually map connections between self-assessments, attack surface management (ASM) results, and certifications like ISO 27001 and SOC 2, thereby revealing hidden dependencies and prioritizing high-risk vectors.

This capability is reflected in successful real-world implementations. For instance, BNP Paribas Personal Finance reduced fraud by 20% using Neo4j's graph-powered detection framework. By moving from siloed data systems to interconnected graph models, the organization was able to visualize and analyze fraud rings in real time. The success hinged on Neo4j's ability to track dynamic relationships across diverse data sources, delivering fast and effective fraud detection through contextual awareness (DKMECO Use Case). This same power of graph modeling can be applied to IoT security, where understanding how devices, vendors, and network segments interrelate is vital for preventing cyber threats [116].

A central challenge in securing IoT deployments is the retained access many manufacturers have to their devices post-deployment, whether for performance monitoring, analytics, or firmware updates. While operationally beneficial, this ongoing access creates persistent entry points for attackers. Regulatory changes such as the U.S. Securities and Exchange Commission's cyber incident reporting rules [46] further intensify the need for transparency and robust cyber risk reporting. To comply, organizations must develop a deep understanding of their vendors' security postures and manage risk continuously.

This makes comprehensive Third-Party Risk Management (TPRM) essential. TPRM involves identifying, assessing, and mitigating risks posed by third-party engagements throughout their lifecycle from procurement to off-boarding [100]. For IoT environments, this entails using diverse data sources: self-assessment questionnaires, due diligence reports, deep-dive audits, and ASM findings. These inputs help establish a robust risk scoring framework that evaluates both individual device-level vulnerabilities and systemic third-party risk.

As demonstrated earlier in the research, Neo4j can be used to enhance TPRM by mapping dependencies among IoT devices, vendors, and network paths, exposing risks traditional models overlook. Attack Surface Management tools like Nessus, Shodan or BitSight feed data into this graph, enabling real-time analysis that highlights discrepancies between vendor self-reports and actual vulnerabilities. This approach is particularly relevant for IoT environments heavily dependent on external components like vendor-supplied sensors or cloud integrations. For instance, an exposed third-party camera vulnerable to CVE-2021-28372 could become a gateway for deeper system compromise—something graph analysis can illuminate by tracing multi-hop threat vectors.

Manufacturing, financial services, utilities, and other sectors have all experienced damaging breaches from supply chain compromises. Connected devices especially those with outdated firmware, weak encryption, or limited vendor support are frequent targets. Effective TPRM must go beyond compliance checklists to address these practical security challenges. Standards like ISO 28000 exist, but real-world adoption remains limited [33]. Moreover, security must be embedded in all stages of the vendor lifecycle as a continuous process. It should not be viewed as a one-time certification or static assessment but as a living system of assurance requiring regular updates and stakeholder consensus [47].

The TPRM lifecycle includes key components such as self-assessments, deep dive evaluations, ASM scans, and due diligence questionnaires. Self-assessments, conducted annually or as needed, align vendor practices with standards like IEC 62443 for industrial control systems [94] and NIST IR 8259 for consumer IoT [66]. Attack Surface Management helps reduce vendor exposure by identifying insecure interfaces such as open APIs or unprotected cloud connections. Deep dive assessments provide in-depth insights into vendor procedures and can be triggered after incidents or due to poor ASM scores. Due diligence questionnaires further scrutinize vendors' provisioning practices, update mechanisms, and use of hardware-based protections. This systematic evaluation ensures only vendors with strong risk hygiene are onboarded.

Ultimately, a strong TPRM strategy grounded in graph-based analysis offers organizations the capability to visualize, prioritize, and mitigate risks dynamically. Certifications such as SOC 2 and ISO 27001 offer evidence of a vendor's security maturity, but it is through continuous and contextual analysis—enabled by tools like Neo4j—that organizations can achieve resilience. This fosters a shared responsibility model in which vendors are held accountable for their security controls and buyers set clear expectations aligned with their risk tolerance. Such alignment is crucial for building trustworthy, secure partnerships in an increasingly interconnected IoT ecosystem.

6.1 How Graph Databases Neo4J Can Enhance Third-Party Risk Management Program

Neo4J is a graph database management system that provides optimized and native graph storage and processing capabilities. In this system, relationships attached to a node directly connect that node to other related nodes. This structure allows for an intuitive and efficient way to traverse the graph. Neo4J is particularly well-suited for dynamic graph data and is effective for modeling and analyzing complex relationships. In this research, Neo4J is used to model and analyze connections between third-party self-assessments, attack surface management (ASM) results, and the availability of ISO27001 and SOC2 certifications. These components together offer insights into evaluating an IoT vendor's security posture.

Neo4J supports dynamic updates, meaning new data can be ingested as it becomes available. This enables a real-time and evolving understanding of vendor security. Its graphical interface also provides a visual overview of relationships and risk patterns, allowing stakeholders to quickly interpret data and make informed decisions. As the complexity of vendor ecosystems grows, the use of Neo4J offers a clear advantage in understanding how different security elements influence one another. The visual structure of the database allows users to follow specific relationships across systems, certifications, and vulnerabilities.

As previously discussed in this research, IoT devices such as Axis cameras and Hikvision systems are increasingly deployed within enterprise networks. However, these integrations often introduce significant security vulnerabilities. For example, CVE-2017-0144, which targeted Windows systems, has been associated with weaknesses exploited through IoT devices. Because these IoT solutions are usually outsourced and composed of interdependent hardware, firmware, and software components, securing them requires a holistic approach. Rather than viewing them in isolation, organizations should adopt a supply chain security perspective.

This means that third-party risk management principles must apply to IoT vendors as well. Vendors must demonstrate their security capabilities before a partnership begins and maintain those standards throughout the product's lifecycle. IoT vendors may introduce risks such as hardcoded credentials, outdated firmware, unpatched vulnerabilities, or insufficient encryption. Therefore, organizations should define and enforce a Third-Party and Outsourcing Risk Policy.

Such a policy should set minimum acceptable security standards to mitigate the risks associated with outsourced IoT deployments.

Due diligence remains central to evaluating a vendor's security posture. This process should be tailored based on each vendor's level of integration and the criticality of their services or products. Vendor self-assessments are a starting point in this process and provide a baseline understanding of a vendor's internal security controls. However, they are limited in scope and cannot always uncover hidden flaws. These assessments might omit technical vulnerabilities or reflect overconfidence in the vendor's own processes.

To address this, external assessments should be conducted, especially for high-risk vendors. This includes vulnerability scans, penetration testing, and attack surface monitoring. Attack surface management is particularly valuable for identifying publicly exposed systems and assessing how these exposures evolve over time. Continuous monitoring supports security compliance by ensuring that changes in the vendor's environment or new threats are rapidly identified. Periodic security audits and external scans should form part of an ongoing due diligence strategy.

Cyber threats are constantly evolving, which means vendor security must also be adaptive. Industries such as finance and healthcare, which are governed by strict regulatory frameworks, require thorough third-party risk management. These industries often mandate self-assessments, independent evaluations, and ongoing monitoring as standard practice. Yet, in many organizations, current vendor assessment methods remain fragmented. Often, they rely on static tools such as spreadsheets or disconnected platforms, lacking the ability to correlate results from different assessments.

To overcome these limitations, this research proposes a Neo4J-based framework to model IoT vendor security posture. This framework will integrate data from self-assessments, due diligence reports, and attack surface analysis into a unified structure. It aims to standardize the evaluation process, allowing decision-makers to understand not just isolated metrics, but how these data points relate within the broader security ecosystem. This approach provides a more complete and structured view of a vendor's security posture. Using Neo4J in this way supports a data-driven, visual, and scalable method for managing third-party IoT risk. It enables proactive responses to emerging risks and supports more informed procurement and security decisions. Ultimately, this framework bridges the gap between disconnected assessment tools

and a unified security analysis model. It ensures that organizations can make decisions with a full understanding of the risks that vendors may introduce.

6.2 Proposed Framework for Evaluating IoT Vendor Security Framework

This research proposes using a graph database (Neo4j) to model TPRM questionnaires data. By isolating security-relevant responses and applying a weighted scoring system, organizations can derive an objective security posture score for each IoT vendor. This facilitates better vendor comparisons, risk ranking, and strategic decision-making in third-party risk management.

This proposed framework introduces the use of a Neo4j graph database to analyze the security posture of IoT vendors, focusing specifically on data derived from third-party risk management (TPRM) questionnaires. The framework isolates only the security-related questions and applies a weighted scoring system to produce a holistic and dynamic view of vendor security. By mapping vendors, their responses, related domains, and certification statuses into a graph structure, organizations can gain deep contextual insights into their risk exposure.

The framework evaluates vendors across multiple dimensions, such as due diligence, deep dive assessments, attack surface management, and self-assessment results. Each of these assessments contributes a weighted score to the vendor's overall security posture. For example, a due diligence score of 70 out of 100 may indicate that the vendor adheres to certain best practices but still has potential gaps in documentation, policies, or procedural maturity. A deeper security evaluation, producing a score of 80 out of 100, reflects stronger foundational controls while still identifying areas for improvement such as incident response or risk management processes.

Attack surface management is assessed independently to evaluate a vendor's external-facing security readiness. A high score in this area, such as 90 out of 100, suggests active monitoring, threat detection, and vulnerability management. This data is represented in the Neo4j model through relationships that define how each score is tied to specific questions, categories, and risk themes. Self-assessment scores, while valuable, are approached cautiously. A high self-reported score of 90 may indicate strong internal confidence in security controls, but the framework acknowledges the potential for bias in such results. As a result, these scores are flagged in the graph for validation against third-party audits or certifications.

Certification status plays a key role in the model. The absence of ISO27001 certification is identified as a risk factor and linked as a negative attribute in the vendor's node. This absence suggests a lack of structured, formalized, and internationally recognized information security governance [43]. On the other hand, the presence of SOC2 certification is treated as a strong indicator of adherence to data protection standards, particularly concerning availability, confidentiality, and integrity of sensitive information. In Neo4j, certifications are attached to vendor nodes with additional properties such as validity period, scope, and issuing authority, enabling robust certification tracking and filtering.

Through Cypher queries, the framework calculates an overall security score per vendor by combining scores and weights assigned to each dimension. Vendors with high aggregated scores are ranked more favorably, while those with inconsistent or missing data are flagged for follow-up. This scoring approach helps prioritize vendors for audits, onboarding decisions, or contract renewals based on their security maturity.

Neo4j's graph structure allows real-time updates, with new questionnaire responses dynamically affecting vendor scores. Each new data point becomes a node or relationship that connects to existing data, enabling continuous posture evaluation. Visualization tools such as Neo4j Bloom provide an intuitive view of the vendor ecosystem, helping stakeholders understand how scores relate to specific security practices and certifications.

The graph model also enables advanced analytics. Algorithms like PageRank or centrality analysis can highlight critical vendors within the organization's supply chain. The framework supports the assignment of custom weights to different security domains, allowing organizations to prioritize based on their industry-specific concerns. For example, a healthcare organization may place greater emphasis on HIPAA-related controls, while a financial institution might prioritize SOC2 and encryption practices [42].

This model tracks posture evolution over time, allowing organizations to detect positive trends or regressions in a vendor's performance. Timestamped relationships help determine whether a vendor is improving or falling behind in its security efforts. Alerts can be generated for vendors that fall below acceptable thresholds, providing early warnings before vulnerabilities are exploited. The Neo4j database can also integrate with external threat intelligence feeds, such as CVE databases, to enhance situational awareness. If a vendor's IoT devices are linked to known vulnerabilities, the graph flags them for immediate review. All data is secured within

Neo4j with strict access controls, protecting sensitive information about vendor performance.This framework is scalable and adaptable. It can accommodate hundreds of vendors and thousands of questionnaire responses while remaining performant and insightful. Though focused solely on security in this research, the model can be extended to include other dimensions such as compliance, privacy, or operational risk. The structured, visual, and data-driven nature of this framework enhances communication with executives and boards by turning complex assessment data into accessible insights. It transforms subjective questionnaire responses into objective security posture evaluations. Ultimately, by using graph database technology, this framework enables smarter, faster, and more informed decisions in managing third-party IoT vendor risk.

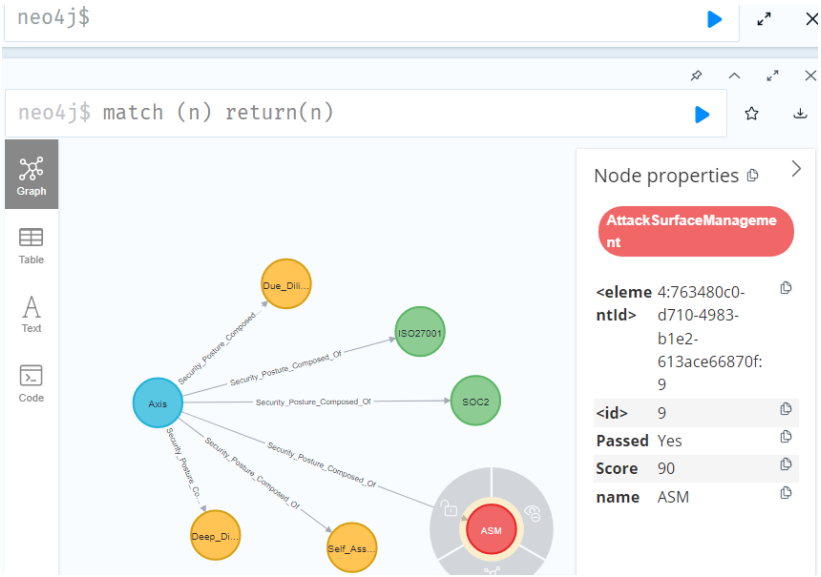

Figure 17. Evaluating IoT suppliers from a TPRM or Third-Party Risk Management perspective

Based on the security posture analysis of IoT vendor “Axis” using Neo4J data, the overall security stance can be inferred from multiple assessments as well as availability of SOC2 and ISO27001 certification. The key observations and their impact on security are as follows:
The combination of strong ASM (90), Self-Assessment (90), and Deep Dive (80) scores suggests that Axis has a relatively strong security posture in terms of practical security defenses and self-evaluation. However, the moderate Due Diligence score (70) and lack of ISO27001

certification indicate that there might be gaps in governance, compliance, or long-term risk management strategies.

The presence of a SOC2 certification compensates for the missing ISO27001 to some extent, ensuring a level of operational security and data protection practices. The lack of ISO27001 suggests that security governance might not be as mature as it could be. If Axis needs to work with enterprise customers or industries requiring strict compliance, obtaining ISO27001 could be beneficial. The high ASM score suggests that Axis has strong external security measures, reducing the risk of cyber threats. The self-assessment score of 90 is strong but should be verified through third-party audits or industry benchmarks to ensure objectivity.

Based on the research findings Axis vendorshould consider improving governance frameworks (potentially adopting ISO27001), closing any policy/process gaps identified in the Due Diligence assessment, and ensuring continuous third-party validation of security measures.

As a conclusion Axis appears to have a strong security posture with good external threat management and operational security practices. However, there are gaps in formalized governance and compliance, which could pose risks in highly regulated environments. Strengthening governance by pursuing ISO27001 or enhancing policy frameworks could make Axis a more trustworthy vendor in the IoT space.

The proposed Neo4j framework enables dynamic security posture scoring of IoT vendors by aggregating weighted assessments from TPRM questionnaires, certifications, and external evaluations. By structuring vendor data as interconnected nodes, the model captures nuanced relationships between security controls, risks, and compliance gaps that traditional methods overlook. To enhance decision-making, the framework can integrate RAG (Red-Amber-Green) status calculations, where thresholds for each color are derived from industry benchmarks or organizational risk appetite. A vendor’s overall score could translate into RAG ratings for example, scores below 50 trigger a "Red" status, 50–75 an "Amber" warning, and above 75 a "Green" approval. These thresholds can be adjusted per domain, such as stricter limits for attack surface management due to its criticality in IoT ecosystems. RAG statuses are dynamically updated as new questionnaire responses or certifications are ingested into the graph, ensuring real-time risk visibility. The calculations can also incorporate contextual modifiers, such as downgrading a vendor to "Amber" if they lack ISO27001 despite a high self-assessment score. Graph traversals automate RAG assignments by comparing scores against predefined risk policies stored as node properties in Neo4j. Relationships in the graph, such as shared vulnerabilities across vendors, can propagate RAG status changes to reflect systemic risks. For

instance, a "Red" rating for a high-risk vendor could trigger reevaluation of connected vendors in the supply chain.

The framework can correlate RAG ratings with external threat feeds, automatically escalating a vendor to "Red" if their devices are linked to active exploits. Conditional logic in Cypher queries supports scenario testing, such as simulating how a new vulnerability would impact RAG distributions. Integrating RAG metrics with centrality algorithms helps identify high-risk vendors that disproportionately affect network security. The graph's flexibility allows organizations to redefine RAG parameters for specific use cases, such as stricter thresholds for healthcare IoT vendors handling PHI. By combining quantitative scoring with qualitative RAG indicators, the framework bridges technical assessments and executive risk communication. Ultimately, RAG-enhanced analytics transform complex vendor data into actionable insights, aligning TPRM processes with operational risk management goals. This approach not only standardizes vendor comparisons but also fosters proactive mitigation of supply chain risks in IoT deployments.

Conclusion

The rapid expansion of IoT ecosystems has introduced complex security challenges that demand innovative approaches to threat modeling and risk management. This thesis has explored these challenges through the lens of Axis surveillance cameras, demonstrating how traditional security frameworks fall short in addressing the interconnected nature of modern IoT vulnerabilities. By integrating graph database technology with established cybersecurity methodologies, this research presents a paradigm shift in how organizations can understand and mitigate risks in their IoT deployments.

The limitations of conventional vulnerability scanning and linear threat assessment models became evident through this investigation. Where traditional methods like STRIDE and DREAD provide static snapshots of potential threats, they fail to capture the dynamic relationships between devices, vulnerabilities, and attack vectors that characterize real-world IoT environments. The research revealed how seemingly minor vulnerabilities such as default credentials in cameras or unpatched firmware in peripheral devices can serve as entry points for sophisticated multi-stage attacks that compromise entire networks.

Neo4j emerged as a powerful solution to these challenges, enabling security teams to visualize and analyze the complex web of relationships within IoT ecosystems. Through graph-based modeling, the study demonstrated how attack paths that would remain invisible to traditional scanners such as lateral movement from a compromised camera to critical servers can be identified and mitigated proactively. The integration of MITRE ATT&CK for IoT provided a structured framework for categorizing these threats and aligning defenses with known adversary tactics.

A key finding of this research is the critical importance of context in IoT security. Where conventional vulnerability management might prioritize issues based solely on CVSS scores, the graph-based approach revealed how factors like device placement, network segmentation, and third-party dependencies dramatically alter risk profiles. This contextual understanding proved particularly valuable in assessing supply chain risks, where vulnerabilities in vendor-provided components could propagate through interconnected systems.

The study also highlighted the value of data visualization in translating technical findings into actionable insights. Power BI dashboards served as a bridge between graph-derived threat intelligence and organizational decision-making, enabling stakeholders to prioritize

remediation efforts based on both technical severity and business impact. This approach addressed a common gap in IoT security programs, the difficulty of communicating complex technical risks to non-technical leadership.

Third-party risk management emerged as another critical area where graph technology offers significant advantages. The research demonstrated how Neo4j can correlate vendor self-assessments with empirical scan data, revealing discrepancies between claimed security postures and actual vulnerabilities. This capability is particularly valuable for IoT ecosystems, where organizations often rely on external vendors for critical components but lack visibility into their security practices.

Looking forward, the findings of this research suggest several important directions for both practice and further study. Security teams should consider graph-based approaches as essential tools for IoT threat modeling, particularly in environments with complex interdependencies. The success of the Neo4j implementation with Axis cameras indicates that similar methodologies could be applied to other IoT device categories, from industrial sensors to medical devices.

Organizations must also recognize that IoT security cannot be treated as an isolated technical challenge. Effective protection requires collaboration across procurement, vendor management, and network architecture teams, with graph models serving as a shared language for understanding systemic risks. The regulatory landscape is beginning to reflect this reality, with emerging standards placing greater emphasis on supply chain security and continuous monitoring.

While this research focused on surveillance cameras, the framework developed here has broader applicability to the IoT security field. The same principles of relationship mapping and contextual risk assessment could be extended to smart cities, connected vehicles, or industrial control systems. Future research could explore these applications while also investigating ways to automate aspects of graph modeling for real-time threat detection.

The evolution of IoT threats shows no signs of slowing, with attackers continually developing new techniques to exploit the growing attack surface. In this environment, static security approaches will prove increasingly inadequate. This thesis demonstrates that graph-based methods offer a more adaptive alternative, one that can keep pace with the complexity of modern IoT ecosystems while providing the actionable intelligence organizations need to protect their networks.

Ultimately, securing IoT environments requires moving beyond the checklist mentality of traditional cybersecurity. By adopting the graph-based framework presented here, organizations can develop a more nuanced understanding of their risk landscape, make better-informed decisions about resource allocation, and build defenses that account for the interconnected nature of contemporary threats. The path forward for IoT security lies not in treating devices as isolated components, but in understanding and securing the complex web of relationships that make up today's digital ecosystems.

This research contributes to that future by providing both a methodological foundation and practical tools for next-generation IoT security. As connected devices continue to proliferate across industries, the approaches developed here will become increasingly essential for organizations seeking to harness the benefits of IoT technology without compromising their security posture. The lessons learned from Axis cameras apply equally to the broader IoT landscape, offering a blueprint for more effective threat modeling and risk management in an interconnected world.

The journey toward secure IoT ecosystems is ongoing, but with graph-based approaches, organizations now have the means to navigate their complexity. By embracing these methods and continuing to refine them through research and practice, we can work toward a future where the promise of IoT innovation is matched by equally sophisticated protections against emerging threats. This thesis represents a step toward that future, demonstrating both the necessity and feasibility of a new approach to IoT security, one grounded in the power of relationships and context to reveal and mitigate risks that traditional methods cannot see.

While this thesis has demonstrated the power of graph-based models for contextualizing IoT vulnerabilities, it also highlights that there is no one-size-fits-all solution for IoT security. No single methodology such as graph modeling, STRIDE/DREAD or TPRM can fully secure IoT ecosystems in isolation. Future research should therefore focus on developing hybrid frameworks that integrate graph technology with TPRM practices, with a strong emphasis on security questionnaires such as self-assessments, due diligence, and other assurance mechanisms such as ISO27001, or SOC 2 Type II reports availability.

The extension of graph databases like Neo4j to model not only technical relationships among IoT devices, but also the broader ecosystem of service providers, compliance obligations, and industry-specific security requirements. For instance, a future system could allow organizations to click on a specific IoT vendor node within the graph and instantly visualize:

- The industry sector they serve (banking, healthcare, manufacturing)
- The certifications required for that sector (PCI DSS for finance, HIPAA for healthcare, ISO/IEC 27001etc.,)
- The questionnaire results or gaps identified during due diligence, yearly self-assessments
- Security assurance artifacts, such as penetration test reports or compliance audits.

This would create a dynamic risk dashboard that ties regulatory context, vendor posture, and technical vulnerabilities into a single, navigable system. Additionally, future studies could explore how automated ingestion of industry standards and vendor documentation (SOC 2 reports, ISO certification details) could populate and update the graph, enabling real-time compliance tracking.

Finally, integration with existing governance, risk, and compliance (GRC) tools could further bridge the gap between high-level risk management and low-level technical data, creating an end-to-end view of IoT security posture that supports both operational and executive decision-making.

References

[1] ‘2.Tele2iot.Com/l/310931/2019-10-30/Fp8ryj/310931/85315/WP_Healthcare_OK.Pdf’. Accessed 11 May 2025. https://2.tele2iot.com/l/310931/2019-10-30/fp8ryj/310931/85315/WP_Healthcare_OK.pdf.

[2] Abrahams, Temitayo Oluwaseun, Sarah Kuzankah Ewuga, Samuel Onimisi Dawodu, Abimbola Oluwatoyin Adegbite, and Azeez Olanipekun Hassan. ‘A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION’. Computer Science & IT Research Journal 5, no. 1 (9 January 2024): 1–25. https://doi.org/10.51594/csitrj.v5i1.699.

[3] Shukla, Piyush Kumar, Aditya Patel, Prashant Kumar Shukla, Prashant Parashar, and Basant Tiwari, eds. IoT in Healthcare Systems: Applications, Benefits, Challenges, and Case Studies. Boca Raton: CRC Press, 2023. https://doi.org/10.1201/9781003145035.

[4] Ouaissa, Mariyam, Mariya Ouaissa, and Zakaria Boulouard, eds. AI and IoT for Proactive Disaster Management. Hershey, PA: IGI Global, 2024.

[5] Sallam, Karam, Mona Mohamed, and Ali Wagdy Mohamed. ‘Internet of Things (IoT) in Supply Chain Management: Challenges, Opportunities, and Best Practices’. Sustainable Machine Intelligence Journal 2 (29 March 2023): (3):1-32. https://doi.org/10.61185/SMIJ.2023.22103.

[6] ‘E-Book - Maximising Business Value Exploring IoT Possibilities in FM.Pdf’. Accessed 11 May 2025. https://planon.showpad.com/share/4o38WyXQSoqWqnGWhZtsD.

[7] Chapple, Mike, James Michael Stewart, and Darril Gibson. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide. Hoboken, New Jersey, 2021.

[8] ‘NVD - Vulnerability Metrics’. Accessed 11 May 2025. https://nvd.nist.gov/vuln-metrics/cvss.

[9] Barki, Amira, Abdelmadjid Bouabdallah, Saïd Gharout, and Jacques Traoré. ‘M2M Security: Challenges and Solutions’. Commun. Surveys Tuts. 18, no. 2 (1 April 2016): 1241–54. https://doi.org/10.1109/COMST.2016.2515516.

[10] Courtney, Peter C. ‘To Render or Intern: Counterterrorism Methods of the FBI SIS and CIA’. International Journal of Intelligence and CounterIntelligence 26, no. 3 (1 September 2013): 482–506. https://doi.org/10.1080/08850607.2013.780553.

[11] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. ‘The Internet of Things: A Survey’. Computer Networks 54, no. 15 (28 October 2010): 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010.

[12] ‘The Three Phases of IoT and OT Security’. Accessed 11 May 2025. https://www.cyberark.com/resources/stream-embed-for-securing-iot-and-ot/the-three-phases-of-iot-and-ot-security-whitepaper.

[13] Secureframe. ‘99+ Essential Third-Party Risk Statistics and Trends for 2024’. Accessed 11 May 2025. https://secureframe.com/blog/third-party-risk-statistics.

[14] Ponemon Institute. ‘The Internet of Things (IoT): A New Era of Third-Party Risk’. Accessed 12 May 2025. https://www.ponemon.org/research/ponemon-library/security/the-internet-of-things-iot-a-new-era-of-third-party-risk.html.

[15] ‘Guide For Cellular IoT Security | Emnify Whitepaper’. Accessed 11 May 2025. https://www.emnify.com/whitepapers/guide-for-cellular-iot-security.

[16] ‘ISO/IEC 27002:2022, Third Edition: Information Security, Cybersecurity and Privacy Protection - Information Security Controls - International Organization For Standardization: 9789267112534 - AbeBooks’. Accessed 11 May 2025. https://www.abebooks.com/9789267112534/ISOIEC-27002-2022-Third-Edition-9267112538/plp.

[17] Trull, J. (2015). Responsible disclosure: Cyber security ethics. CSO Online. https://www.csoonline.com/article/2889357/responsibledisclosure-cyber-security-ethics.html

[18] ‘2 Million IoT Security Cameras and Baby Monitors Vulnerable to Takeover’, 29 April 2019. https://threatpost.com/iot-devices-vulnerable-takeover/144167/.

[19] Cohen, Doron Voolf, Sara Boddy, Remi. ‘Gafgyt Targeting Huawei and Asus Routers and Killing Off Rival IoT Botnets’. F5 Labs, 26 December 2019. https://www.f5.com/labs/articles/threat-intelligence/gafgyt-targeting-huawei-and-asus-routers-and-killing-off-rival-iot-botnets.

[20] ‘The Vulnerability Disclosure Process: Still Broken’, 5 September 2018. https://threatpost.com/the-vulnerability-disclosure-process-still-broken/137180/.

[21] Zetter, Kim. ‘A Bizarre Twist in the Debate Over Vulnerability Disclosures’. Wired. Accessed 11 May 2025. https://www.wired.com/2015/09/fireeye-enrw-injunction-bizarre-twist-in-the-debate-over-vulnerability-disclosures/.

[22] ZDNET. ‘Researcher Publishes Second Steam Zero Day after Getting Banned on Valve’s Bug Bounty Program’. Accessed 11 May 2025. https://www.zdnet.com/article/researcher-publishes-second-steam-zero-day-after-getting-banned-on-valves-bug-bounty-program/.

[23] Algarni, Abdullah M, and Yashwant K Malaiya. ‘Software Vulnerability Markets: Discoverers and Buyers’ 8, no. 3 (2014).

[24] Stifter, Nicholas, Aljosha Judmayer, Philipp Schindler, Alexei Zamyatin, and Edgar Weippl. ‘Agreement with Satoshi – On the Formalization of Nakamoto Consensus’, 2018. Cryptology ePrint Archive. https://eprint.iacr.org/2018/400.

[25] Fotiou, Nikos, and George C. Polyzos. ‘Smart Contracts for the Internet of Things: Opportunities and Challenges’. 2018 European Conference on Networks and Communications (EuCNC), June 2018, 256–60. https://doi.org/10.1109/EuCNC.2018.8443212.

[26] Fagan, Michael, Katerina Megas, Karen Scarfone, and Matthew Smith. ‘Foundational Cybersecurity Activities for IoT Device Manufacturers’. National Institute of Standards and Technology, 29 May 2020. https://doi.org/10.6028/NIST.IR.8259.

[27] James. ‘The IoTSF Publishes a New Best Practice Guide on IoT Cybersecurity for Facilities Professionals in the Smart Built Environment’. IoT Security Foundation (blog), 30 March 2023. https://iotsecurityfoundation.org/the-iotsf-publishes-a-new-best-practice-guide-on-iot-cybersecurity-for-facilities-professionals-in-the-smart-built-environment/.

[28] Dahmen-Lhuissier, Sabine. ‘Consumer IoT Security’. ETSI. Accessed 12 May 2025. https://www.etsi.org/technologies/consumer-iot-security.

[29] ‘IoT Security: How to Protect Your Connected Devices | Wattlecorp Cybersecurity Labs’, 28 April 2024. https://www.wattlecorp.com/iot-security/.

[30] Sebestyen, Hannelore, Daniela Elena Popescu, and Rodica Doina Zmaranda. ‘A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories’. Computers 14, no. 2 (February 2025): 61. https://doi.org/10.3390/computers14020061.

[31] ISO. ‘ISO 28000:2007’. Accessed 11 May 2025. https://www.iso.org/standard/44641.html.

[32] Industry IoT Consortium. ‘Industrial Internet Security Framework’. Accessed 11 May 2025. https://www.iiconsortium.org/iisf/.

[33] Soldatos, John, ed. Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection. Now Publishers, 2020. https://doi.org/10.1561/9781680836837.

[34] Gamble, Grant. ‘The Future of Data Visualization with Power BI’. Medium (blog), 7 December 2024. https://medium.com/@powerbicourses/the-future-of-data-visualization-with-power-bi-f5425a34daa9.

[35] Lippmann, R. P., and K. W. Ingols. ‘An Annotated Review of Past Papers on Attack Graphs’. Accessed 11 May 2025. https://apps.dtic.mil/sti/citations/ADA431826.

[36] Oct 16 and 2019. ‘Impacts of Cyberattacks on IoT Devices’. Palo Alto Networks. Accessed 11 May 2025. https://www.paloaltonetworks.com/resources/research/impacts-of-cyberattacks-on-iot-devices.

[37] Peltier, Thomas R. Information Security Risk Analysis. 1st edition. Boca Raton, Fla.: Auerbach Publications, 2001.

[38] Ketel, Mohammed. ‘IT Security Risk Management’. In Proceedings of the 46th Annual ACM Southeast Conference, 373–76. ACMSE ’08. New York, NY, USA: Association for Computing Machinery, 2008. https://doi.org/10.1145/1593105.1593203.

[39] ‘Risk Management - Principles and Inventories for Risk Management / Risk Assessment Methods and Tools | ENISA’. Accessed 11 May 2025. https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools.

[40] KPMG. ‘Outsourcing and Third Party Risk Management’. Accessed 11 May 2025. https://kpmg.com/uk/en/insights/regulatory/outsourcing-and-third-party-risk-management.html.

[41] James. ‘The IoTSF Publishes a New Best Practice Guide on IoT Cybersecurity for Facilities Professionals in the Smart Built Environment’. IoT Security Foundation (blog), 30 March 2023. https://iotsecurityfoundation.org/the-iotsf-publishes-a-new-best-practice-guide-on-iot-cybersecurity-for-facilities-professionals-in-the-smart-built-environment/.

[42] Secureframe. ‘SOC 2 Report’. Accessed 11 May 2025. https://secureframe.com/hub/soc-2/report.

[43] ‘Vendor Risk Assessment for ISO 27001 Requirements | Bitsight’. Accessed 11 May 2025. https://www.bitsight.com/blog/vendor-risk-assessment-iso-27001-requirements.

[44] Kauffman, Sharon. ‘Vulnerability Assessment in Third-Party Risk Management’. Northdoor (blog), 18 March 2024. https://www.northdoor.co.uk/insight/blog/the-importance-of-vulnerability-assessment-in-tprm/.

[45] Asimily. ‘Managing Third-Party IoT Security Risk’, 8 May 2024. https://asimily.com/blog/managing-third-party-iot-security-risk/.

[46] PricewaterhouseCoopers. ‘SEC’s Cyber Disclosure Rule’. PwC, 2 April 2024. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules.html.

[47] ‘Baseline Security Recommendations for IoT | ENISA’, 21 February 2024. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[48] Azrour, Mourade, Jamal Mabrouki, Azidine Guezzaz, and Ambrina Kanwal. ‘Internet of Things Security: Challenges and Key Issues’. Security and Communication Networks 2021, no. 1 (2021): 5533843. https://doi.org/10.1155/2021/5533843.

[49] Choo, Kim-Kwang Raymond, Rongxing Lu, Liqun Chen, and Xun Yi. ‘A Foggy Research Future: Advances and Future Opportunities in Fog Computing Research’. Future Generation Computer Systems 78 (1 January 2018): 677–79. https://doi.org/10.1016/j.future.2017.09.014.

[50] Rashid, Suhaila Abdul, Mohammad Hussaini Wahab, Wan Nurul Mardiah Wan Mohd. Rani, and Syuhaida Ismail. ‘Safety of Street: The Role of Street Design’. AIP Conference Proceedings 1891, no. 1 (3 October 2017): 020008. https://doi.org/10.1063/1.5005341.

[51] Abu Bakar, Nur Azaliah, Wan Makhtariah, and Noor Hassan. ‘The Internet of Things in Healthcare: Anoverview, Challenges and Model Plan for Security Risks Management Process’. Indonesian Journal of Electrical Engineering and Computer Science 15 (1 July 2019): 414–20. https://doi.org/10.11591/ijeecs.v15.i1.pp414-420.

[52] Sadoian, Leah. ‘Vendor Due Diligence Questionnaire (Free Template) | UpGuard’. Accessed 11 May 2025. https://www.upguard.com/blog/vendor-due-diligence-questionnaires-free-template.

[53] Neo4j Graph Data Platform. ‘Using the Neo4j BI Connector - Neo4j Aura’. Accessed 12 May 2025. https://neo4j.com/docs/aura/classic/tutorials/bi/.

[54] ‘Managing Internet of Things Devices With Third-Party Risk Management’. Accessed 11 May 2025. https://www.venminder.com/blog/manage-internet-of-things-devices-third-party-risk-management.

[55] Team, SaltyCloud Research. ‘ISRM: What Are Self-Assessment Questionnaires (SAQs)?’ Isora GRC (blog), 4 March 2024. https://www.saltycloud.com/blog/isrm-what-are-self-assessment-questionnaires-saqs/.

[56] ‘A Basic Risk Assessment and Management Method’. Accessed 11 May 2025. https://www.ncsc.gov.uk/collection/risk-management/a-basic-risk-assessment-and-management-method.

[57] ‘AXIS OS Knowledge Base’. Accessed 11 May 2025. https://help.axis.com/en-us/axis-os-knowledge-base.

[58] ‘Axis: 90% Of Hacks Are NOT The Manufacturer’s Fault - IPVM Discussions’. Accessed 11 May 2025. https://ipvm.com/discussions/axis-90-of-hacks-are-not-the-manufacturer-s-fault.

[59] Malge, Sunilkumar, and Pallavi Singh. ‘Internet of Things IoT: Security Perspective’. International Journal of Trend in Scientific Research and Development Volume-3 (30 June 2019): 1041–43. https://doi.org/10.31142/ijtsrd24010.

[60] CrowdStrike.com. ‘Internet of Things (IoT) Security’. Accessed 11 May 2025. https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/internet-of-things-iot-security/.

[61] Moy, Allison. ‘The Importance of IoT Security in a Connected World’. IEEE Innovation at Work (blog), 24 October 2023. https://innovationatwork.ieee.org/the-importance-of-iot-security-in-a-connected-world/.

[62] Jurcut, A., T. Niculcea, P. Ranaweera, and A. LeKhac. ‘Security Considerations for Internet of Things: A Survey’. SN Computer Science 1, no. 4 (July 2020): 193. https://doi.org/10.1007/s42979-020-00201-3.

[63] Soldatos, John, ed. Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection. Now Publishers, 2020. https://doi.org/10.1561/9781680836837.

[64] ‘MITRE ATT&CK®’. Accessed 11 May 2025. https://attack.mitre.org/.

[65] Shodan. ‘Shodan’. Accessed 11 May 2025. https://www.shodan.io.

[66] Fagan, Michael, Katerina Megas, Karen Scarfone, and Matthew Smith. ‘IoT Device Cybersecurity Capability Core Baseline’. National Institute of Standards and Technology, 29 May 2020. https://doi.org/10.6028/NIST.IR.8259A.

[67] ‘Axis Cloud Connect | Axis Communications’. Accessed 11 May 2025. https://www.axis.com/solutions/axis-cloud-connect.

[68] WhatIs. ‘CrowdStrike Outage Explained: What Caused It and What’s next’. Accessed 11 May 2025. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.

[69] ‘What Is Cyber Espionage? | CrowdStrike’. Accessed 12 May 2025. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/.

[70] Tenable®. ‘Tenable Research Advisory: AXIS Camera App Malicious Package Distribution Weakness’, 12 April 2018. https://www.tenable.com/blog/tenable-research-advisory-axis-camera-app-malicious-package-distribution-weakness.

[71] El Hakim, Ahmed. Internet of Things (IoT) System Architecture and Technologies, White Paper., 2018. https://doi.org/10.13140/RG.2.2.17046.19521.

[72] ‘Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®’. Accessed 12 May 2025. https://attack.mitre.org/techniques/T1190/.

[73] CIS. ‘Blog | The Mirai Botnet - Tips to Defend Your Organization’, 29 July 2021. https://www.cisecurity.org/blog/the-mirai-botnet-threats-and-mitigations/.

[74] Bevington, David Atch, Gil Regev, Ross. ‘How to Proactively Defend against Mozi IoT Botnet’. Microsoft Security Blog (blog), 19 August 2021. https://www.microsoft.com/en-us/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/.

[75]Trend Micro. ‘VPNFilter Two Years Later: Routers Still Compromised’, 19 January 2021. https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html.

[76] Trend Micro. ‘Persirai: New IoT Botnet Targets IP Cameras’, 9 May 2017. https://www.trendmicro.com/en_us/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html.

[77] ‘BrickerBot Malware Emerges, Permanently Bricks IoT Devices | Trend Micro (US)’. Accessed 11 May 2025. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/brickerbot-malware-permanently-bricks-iot-devices.

[78] https://digitaldirections.com/. ‘What Are the Main Components of IoT? - Digital Directions’. Accessed 11 May 2025. https://digitaldirections.com/main-components-of-iot/.

[79] Abbas, Mohamed. ‘Monetizing The Internet of Things (IoT)’. 5G HUB TECHNOLOGIES (blog), 1 September 2021. https://5ghub.us/monetizing-the-internet-of-things-iot/.

[80] ‘OWASP IoT Top 10 Vulnerabilities (2025Updated) | Wattlecorp Cybersecurity Labs’, 5 July 2024. https://www.wattlecorp.com/owasp-iot-top-10/.

[81] Gamble, G . ‘The Role of Power BI in Risk Management: Identifying and Mitigating Risks’. Medium, 24 November 2024. https://medium.com/@powerbicourses/the-role-of-power-bi-in-risk-management-identifying-and-mitigating-risks-812f0a3df07b.

[82] ‘Exploitable Vulnerabilities Report - Nessus Report | Tenable®’. Accessed 11 May 2025. https://www.tenable.com/nessus-reports/exploitable-vulnerabilities-report.

[83] ‘Plugins’. Accessed 11 May 2025. https://www.tenable.com/plugins.

[84] Kesselman, Yitzhak, Paddy Osborne, Matt Neely, Tony Bencic, Srinivasan Turuvekere, and CristianCristian Petculescu. ‘Power BI Security White Paper - Power BI’. Accessed 11 May 2025. https://learn.microsoft.com/en-us/power-bi/guidance/whitepaper-powerbi-security.

[85] Kim, Kyoung Ho, Kyounggon Kim, and Huy Kang Kim. ‘STRIDE-Based Threat Modeling and DREAD Evaluation for the Distributed Control System in the Oil Refinery’. ETRI Journal 44, no. 6 (2022): 991–1003. https://doi.org/10.4218/etrij.2021-0181.

[86] ‘Software Secured | Comparison of STRIDE, DREAD & PASTA | USA’. Accessed 11 May 2025. https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta.

[87] Protopsaltis, Antonis, Panagiotis Sarigiannidis, Dimitrios Margounakis, and Anastasios Lytos. ‘Data Visualization in Internet of Things: Tools, Methodologies, and Challenges’. In Proceedings of the 15th International Conference on Availability, Reliability and Security, 1–11. ARES ’20. New York, NY, USA: Association for Computing Machinery, 2020. https://doi.org/10.1145/3407023.3409228.

[88] Nurse, Jason, Sadie Creese, and David Roure. ‘Security Risk Assessment in Internet of Things Systems’. IT Professional 19 (1 September 2017). https://doi.org/10.1109/MITP.2017.3680959.

[89] Computer Security Division, Information Technology Laboratory. ‘About the RMF - NIST Risk Management Framework | CSRC | CSRC’. CSRC | NIST, 30 November 2016. https://csrc.nist.gov/projects/risk-management/about-rmf.

[90] Dubois, Éric, Patrick Heymans, Nicolas Mayer, and Raimundas Matulevičius. ‘A Systematic Approach to Define the Domain of Information System Security Risk Management’. In Intentional Perspectives on Information Systems Engineering, edited by Selmin Nurcan, Camille Salinesi, Carine Souveyet, and Jolita Ralyté, 289–306. Berlin, Heidelberg: Springer, 2010. https://doi.org/10.1007/978-3-642-12544-7_16.

[91] University of Tartu, Faculty of Science and Technology. Institute of Computer Science. (2024, June).Analysis of cyber security risks and mitigation options for automated systems and technologies. https://www.ria.ee/sites/default/files/documents/2024-06/Analysis-of-Cyber-Security-Risks-and-Mitigation-Options-for-Automated-Systems-and-Technologies.pdf

[92] Ganji, Daniel, Christos Kalloniatis, H. Mouratidis, and Saeed Malekshahi Gheytassi. ‘Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review’, 2020. https://www.semanticscholar.org/paper/Approaches-to-Develop-and-Implement-ISO-IEC-27001-A-Ganji-Kalloniatis/5e6fcb8fb166884439c24802709c1fce9ac1bd21.

[93] Approaches to develop and implement ISO/IEC 27001 standard - Information security management systems: A systematic literature review. [PDF]. International Journal on Advances in Software, vol 12 no 3& 4 (2019) http://www.iariajournals.org/software/ ‘IARIA Journals’. Accessed 12 May 2025. http://www.iariajournals.org/software/.

[94] isa.org. ‘ISA/IEC 62443 Series of Standards - ISA’. Accessed 11 May 2025. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[95] Microsoft. (2016). Threat Modeling Tool 2016. https://www.microsoft.com/en-us/download/details.aspx?id=49168

[96] ‘Using the MITRE ATT&CK Framework to Accelerate & Simplify OT/IoT Threat Response’. Accessed 12 May 2025. https://www.nozominetworks.com/blog/using-mitre-attack-for-ics-framework.

[97] (2023). 5 advantages of outsourcing the Internet of Things. LinkedIn. https://www.linkedin.com/pulse/5-advantages-outsourcing-internet-things-kvytech/

[98] Shivanandhan, Manish. ‘How to Exploit the EternalBlue Vulnerability on Windows- A Step-by-Step Guide’. Medium, 18 March 2025. https://blog.stealthsecurity.sh/how-to-exploit-the-eternalblue-vulnerability-on-windows-a-step-by-step-guide-0d9d90b6397c.

[99] ‘Smb-Vuln-Ms17-010 NSE Script — Nmap Scripting Engine Documentation’. Accessed 11 May 2025. https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.

[100] BlueVoyant. (n.d.). What is third-party risk management (TPRM) and what are its objectives? https://www.bluevoyant.com/knowledge-center/third-party-risk-management-tprm-a-complete-guide

[101] Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.

[102] Sacchetti, T., Bognar, M., de Meulemeester, J., et al. (2024). AttackDefense Framework (ADF): Enhancing IoT devices and lifecycles threat modeling [Preprint]. HAL. https://hal.science/hal-04735344v1/file/3698396.pdf

[103] Fang, Zheng, Hao Fu, Tianbo Gu, Pengfei Hu, Jinyue Song, Trent Jaeger, and Prasant Mohapatra. ‘Towards System-Level Security Analysis of IoT Using Attack Graphs’. IEEE Transactions on Mobile Computing 23, no. 2 (February 2024): 1142–55. https://doi.org/10.1109/TMC.2022.3231567.

[104] OWASP. (n.d.). Vulnerability scanning tools. https://owasp.org/www-community/Vulnerability_Scanning_Tools

[105] Nguyen, Dang Tu, Chengyu Song, Zhiyun Qian, Srikanth V. Krishnamurthy, Edward J. M. Colbert, and Patrick McDaniel. 'IoTSan: Fortifying the Safety of IoT Systems'. In Proceedings of the 14th International Conference on Emerging Networking EXperiments and Technologies, 191–203, 2018. https://doi.org/10.1145/3281411.3281440.

[106] Celik, Z. Berkay, Patrick McDaniel, and Gang Tan. 'SOTERIA: Automated IoT Safety and Security Analysis'. In Proceedings of the 2018 USENIX Conference on Usenix Annual Technical Conference, 147–58. USENIX ATC '18. USA: USENIX Association, 2018.

[107] Ding, W., & Hu, H. (2018). On the safety of IoT device physical interaction control. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security.

[108] Wang, Qi, Pubali Datta, Wei Yang, Si Liu, Adam Bates, and Carl A. Gunter. 'Charting the Attack Surface of Trigger-Action IoT Platforms'. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 1439–53. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019. https://doi.org/10.1145/3319535.3345662.

[109] Brezolin, Uelinton, Andressa Vergütz, and Michele Nogueira. 'A Method for Vulnerability Detection by IoT Network Traffic Analytics'. Ad Hoc Networks 149 (1 October 2023): 103247. https://doi.org/10.1016/j.adhoc.2023.103247.

[110] 'NVD - CVE-2019-17627'. Accessed 12 May 2025. https://nvd.nist.gov/vuln/detail/CVE-2019-17627.

[111] 'NVD - CVE-2019-5035'. Accessed 11 May 2025. https://nvd.nist.gov/vuln/detail/CVE-2019-5035.

[112] 'Target Hackers Broke in Via HVAC Company – Krebs on Security', 9 February 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

[113] ‘NVD - Vulnerability Metrics’. Accessed 11 May 2025. https://nvd.nist.gov/vuln-metrics/cvss.

[114] ‘NVD - CVSS v2.0 Calculator’. Accessed 11 May 2025. https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator.

[115] ‘NVD - CVSS v3 Calculator’. Accessed 11 May 2025. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

[116] ‘BNP Paribas Personal Finance Reduces Fraud by 20% with Neo4j’s Graph-Powered Fraud Detection - DKM’, 15 April 2025. https://www.dkmeco.com/en/bnp-paribas-personal-finance-reduces-fraud-by-20-with-neo4js-graph-powered-fraud-detection/.

[117] Chen, Feng, Jinshu Su, and Yi Zhang. ‘A Scalable Approach to Full Attack Graphs Generation’. In Proceedings of the 1st International Symposium on Engineering Secure Software and Systems, 150–63. ESSoS ’09. Berlin, Heidelberg: Springer-Verlag, 2009. https://doi.org/10.1007/978-3-642-00199-4_13.

[118] Sheyner, O., J. Haines, S. Jha, R. Lippmann, and J.M. Wing. ‘Automated Generation and Analysis of Attack Graphs’. In Proceedings 2002 IEEE Symposium on Security and Privacy, 273–84, 2002. https://doi.org/10.1109/SECPRI.2002.1004377

[119] Ammann, Paul, Duminda Wijesekera, and Saket Kaushik. Scalable, Graph-Based Network Vulnerability Analysis. Proceedings of the ACM Conference on Computer and Communications Security, 2002. https://doi.org/10.1145/586110.586140.

[120] Salayma, Marwa. ‘Threat Modelling in Internet of Things (IoT) Environments Using Dynamic Attack Graphs’. Frontiers in the Internet of Things 3 (30 May 2024). https://doi.org/10.3389/friot.2024.1306465.

[121] ‘Take the Neo4j Fundamentals Course with Neo4j GraphAcademy’. Accessed 12 May 2025. https://graphacademy.neo4j.com/courses/neo4j-fundamentals/.

[122] Neo4j Graph Data Platform. ‘Using the Neo4j BI Connector - Neo4j Aura’. Accessed 12 May 2025. https://neo4j.com/docs/aura/classic/tutorials/bi/.

[123] Yan, Peizhi, and Tala Talaei Khoei. ‘Securing the Internet of Things: A Comprehensive Review of Ransomware Attacks, Detection, Countermeasures, and Future Prospects’. Franklin Open 11 (1 June 2025): 100256. https://doi.org/10.1016/j.fraope.2025.100256.

[124] National Cyber Security Centre (NCSC). (2020, June). Ransomware: Measures for preventing a ransomware attack (Fact sheet F5-2020-03, Version 1.0). Ministry of Justice and Security, Netherlands. https://english.ncsc.nl/binaries/ncsc-en/documenten/factsheets/2020/june/30/factsheet-ransomware/71059_NCSC_FS+Ransomeware+EN_WEB.pdf

[125] Uberoi, Aditi. ‘Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About!’ Accessed 11 May 2025. https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about.

License

Non-exclusive licence to reproduce the thesis and make the thesis public

I, Natalja Kjaernested, grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright, my thesis - IoT security: Graph-based vulnerability and risk assessment models, supervised by Sedat Akleylek.

2. I grant the University of Tartu a permit to make the thesis specified in point 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 4.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in points 1 and 2.

4. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Natalja Kjaernested
15.05.2025