Security management model for IoT devices based on international standards

Modelo de gestión de seguridad para dispositivos IoT basado en estándares internacionales

Modelo de gestão de segurança para dispositivos IoT baseado em padrões internacionais

Edwin Javier Collazos Sandoval[1]
Katerine Marceles Villalba[2]
Siler Amador Donado[3]

Received: September 20th, 2024
Accepted: December 10th, 2024
Available: January 20th, 2025

How to cite this article:
E.J. Collazos Sandoval, K. Marceles Villalba, and S. Amador Donado, "Security Management Model for IoT Devices Based on International Standards," *Revista Ingeniería Solidaria,* vol. 21, no. 1, 2025.
doi: https://doi.org/10.16925/2357-6014.2025.01.06

Research article. https://doi.org/10.16925/2357-6014.2025.01.06

[1] Ingeniero Informático, Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca, Popayán, Colombia.
Email: javier@unimayor.edu.co
ORCID: https://orcid.org/0009-0001-3828-776X
CvLAC: https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0002070105

[2] Magíster en Seguridad Informática, Facultad de Ingeniería, Universidad de Antioquia, Medellín, Colombia.
Email: katerine.marceles@udea.edu.co
ORCID: https://orcid.org/0000-0002-4571-0714
CvLAC: https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0001492988

[3] PhD (c) en Ciencias de la Computación, Facultad de Ingeniería, Universidad del Cauca, Popayán, Colombia.
Email: samador@unicauca.edu.co
ORCID: https://orcid.org/0000-0002-4571-8273
CvLAC: https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0000246360

Abstract

Introduction: The research was conducted with the support of the Universidad del Cauca, the Institución Universitaria Colegio Mayor del Cauca, and the Universidad de Antioquia during the year 2023.

Problem: The rapid increase in IoT devices has created a gap in terms of security, as many devices lack adequate protection mechanisms, exposing them to critical vulnerabilities such as weak authentication, unencrypted data transmission, and lack of update management.

Objective: To design a security management model for IoT devices based on international standards that mitigates risks associated with specific vulnerabilities and provides clear guidelines for implementing effective protection measures.

Methodology: The methodology included a systematic literature review, classification of standards, and development of the model at three levels: device security, network security, and security management.

Results: The results highlight the importance of encryption, network segmentation, and regulatory compliance to strengthen security in IoT environments

Conclusion: The developed security management model significantly improves the protection of IoT devices, providing an effective structure based on international standards. Additionally, future developments are proposed, such as integrating artificial intelligence and enhancing user awareness campaigns.

Originality: The model's approach integrates international standards with specific practical measures to address critical IoT vulnerabilities, standing out as an advancement in the field of IoT cybersecurity.

Limitations: The model was tested in a controlled environment and may require adjustments for broader or specific contexts. Additionally, its practical implementation may depend on technical and human resources that not all organizations possess.

Keywords: Authentication Device, International Standards, IoT Security, Security Management, Threat Detection.

Resumen

Introducción: La investigación se llevó a cabo con el apoyo de la Universidad del Cauca, la Institución Universitaria Colegio Mayor del Cauca y la Universidad de Antioquia durante el año 2023.

Problema: El rápido aumento de dispositivos IoT ha generado una brecha en términos de seguridad, ya que muchos dispositivos carecen de mecanismos de protección adecuados, exponiéndolos a vulnerabilidades críticas como autenticación débil, transmisión de datos no cifrados y falta de gestión de actualizaciones.

Objetivo: Diseñar un modelo de gestión de seguridad para dispositivos IoT basado en estándares internacionales que permita mitigar los riesgos asociados con vulnerabilidades específicas y proporcionar directrices claras para la implementación de medidas de protección efectivas.

Metodología: La metodología incluyó una revisión sistemática de la literatura, clasificación de estándares y desarrollo del modelo en tres niveles: seguridad del dispositivo, seguridad de la red y gestión de la seguridad.

Resultados: Los resultados destacan la importancia de la encriptación, segmentación de redes y cumplimiento normativo para fortalecer la seguridad en entornos IoT.

Conclusión: El modelo de gestión de seguridad desarrollado mejora significativamente la protección de dispositivos IoT, proporcionando una estructura efectiva basada en estándares internacionales. Además, se proponen futuros desarrollos como la integración de inteligencia artificial y el perfeccionamiento de campañas de concienciación para usuarios finales.

Originalidad: El enfoque del modelo integra estándares internacionales con medidas prácticas específicas para abordar vulnerabilidades críticas en IoT, destacándose como un avance en el campo de la ciberseguridad aplicada al IoT.

Limitaciones: El modelo fue probado en un entorno controlado y podría requerir ajustes para contextos más amplios o específicos. Además, la implementación práctica puede depender de recursos técnicos y humanos que no todas las organizaciones poseen.

Palabras claves: Autenticación del dispositivo, estándares internacionales, Detección de amenazas, Gestion de seguridad, Seguridad en la IoT.

Resumo

Introdução: Esta pesquisa foi realizada com o apoio da Universidade do Cauca, da Instituição Universitária Colegio Mayor del Cauca e da Universidade de Antioquia durante o ano de 2023.

Problema: O rápido aumento no número de dispositivos de IoT criou uma lacuna de segurança, visto que muitos dispositivos carecem de mecanismos de proteção adequados, expondo-os a vulnerabilidades críticas, como autenticação fraca, transmissão de dados não criptografada e falta de gerenciamento de atualizações.

Objetivo: Projetar um modelo de gerenciamento de segurança para dispositivos de IoT baseado em padrões internacionais que mitigue os riscos associados a vulnerabilidades específicas e forneça diretrizes claras para a implementação de medidas de proteção eficazes.

Metodologia: A metodologia incluiu uma revisão sistemática da literatura, classificação de padrões e desenvolvimento de modelos em três níveis: segurança de dispositivos, segurança de rede e gerenciamento de segurança.

Resultados: Os resultados destacam a importância da criptografia, segmentação de rede e conformidade regulatória para fortalecer a segurança em ambientes de IoT. Conclusão: O modelo de gerenciamento de segurança desenvolvido melhora significativamente a proteção de dispositivos de IoT, fornecendo uma estrutura eficaz baseada em padrões internacionais. Além disso, são propostos desenvolvimentos futuros, como a integração de inteligência artificial e o aprimoramento de campanhas de conscientização para usuários finais.

Originalidade: A abordagem do modelo integra padrões internacionais com medidas práticas específicas para lidar com vulnerabilidades críticas em IoT, destacando-se como um avanço no campo da cibersegurança em IoT.

Limitações: O modelo foi testado em ambiente controlado e pode exigir ajustes para contextos mais amplos ou específicos. Além disso, a implementação prática pode depender de recursos técnicos e humanos que nem todas as organizações possuem.

Palavras-chave: Autenticação de dispositivos, padrões internacionais, Detecção de ameaças, Gestão de segurança, Segurança em IoT.

1. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most significant technological innovations of recent decades, transforming various industries and enhancing operational efficiency through the interconnection of devices. It is estimated that by 2025, there will be over 30 billion IoT devices connected globally, highlighting the magnitude and potential impact of this technology [1]. However, this exponential growth also brings significant security challenges, as many IoT devices lack adequate protection

measures, making them vulnerable to cyberattacks and putting data privacy and integrity at risk [2].

IoT devices encompass a wide range of applications, from smart home devices to industrial systems and applications in healthcare and defense. Despite the benefits IoT offers, security has been a persistent concern. Previous studies have shown that many IoT implementations do not include robust security mechanisms from their design phase [3]. The lack of specific security standards for IoT has led to situations where devices are easily compromised, causing significant damage both at the individual and organizational levels [4]. Existing literature highlights several IoT-related security incidents, such as the DDoS attack using the Mirai botnet, which compromised thousands of IoT devices and affected large-scale services [5]. These incidents underscore the urgent need to develop and adopt security management models that align with international standards and best practices [6].

The growing adoption of IoT devices in critical sectors, such as healthcare and transportation, makes the security of these devices a priority. The lack of a standardized security framework not only exposes devices to attacks but can also result in data loss, service interruptions, and physical safety risks [7]. According to Khan et al., the architecture of IoT and its possible applications present key challenges that must be addressed to ensure user security and privacy [8]. Therefore, it is crucial to develop a security management model that addresses the specific vulnerabilities of IoT devices and is based on recognized international standards [9]. The objective of this study is to design a security management model for IoT devices based on international standards. This model aims to mitigate the risks associated with IoT security by providing clear guidelines for implementing effective protection measures [10].

The development of the security management model was carried out through a systematic literature review and the classification of international standards and best practices [11]. Qualitative methods were used to analyze existing reference frameworks, and a cohesive model was generated, adapted to the security needs of IoT devices [12].

In line with this, the article is organized as follows: the introduction section presents the problem, justification, objectives, and methodological approach of the study. The methodology section describes the systematic literature review process, the classification of standards, and the development of the security management model. The results and discussion section presents the study's findings, including the identification of vulnerabilities and the evaluation of standards, followed by the proposed security management model. Finally, the conclusions section summarizes

the key findings and offers recommendations for future research and the practical implementation of the model

2. METHODOLOGY

The development of the security management model for IoT devices was carried out through three stages: data collection, analysis and synthesis, and model development. Each of these stages is described below.

2.1. Data Collection

A review of existing IoT security literature was conducted, including journal articles, conference papers, international standards, and technical documents, to identify current practices and challenges. [10]. The academic databases included were IEEE Xplore, ACM Digital Library, and Google Scholar, among others. Keywords such as "IoT security," "IoT security standards," and "IoT vulnerabilities" were used.

2.2. Analysis and Synthesis

Once the literature was collected, the information was analyzed and synthesized. This stage included:

- **Classification of Standards and Best Practices:** Identification and categorization of relevant international standards, such as ISO/IEC 27001 and NIST SP 800-183 [11], along with best practices recommended by leading organizations in information security.
- **Identification of Vulnerabilities:** Analysis of common vulnerabilities in IoT devices, based on previous studies and security incident reports. This analysis helped clarify the weak points that the security management model must address [5].
- **Evaluation of Technologies and Protocols:** Review of current IoT security technologies and protocols, assessing their effectiveness across different IoT contexts and device types [6].

e-ISSN 2357-6014 / Vol. 21, no. 1 / january-april 2025 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

2.3. Model Development

Using the analyzed and synthesized information, we developed the security management model. This stage involved:

- **Model Design:** The model was structured into different levels, covering protection from individual devices to entire IoT networks [9].
- **Model Validation:** Case studies assessed the model's ability to mitigate risks and manage security incidents across different IoT scenarios [12].
- **Documentation and Guidelines:** We developed clear guidelines for implementing the model in real-world environments, including practical recommendations for manufacturers, developers, and IoT system administrators [7].

3. RESULTS

This section presents the results obtained through the three stages of the methodological approach: data collection, analysis and synthesis, and development of the security management model for IoT devices.

3.1. Data Collection

During the data collection stage, we reviewed over 100 academic journal articles, technical documents, and international standards. This process identified the main vulnerabilities and challenges in IoT device security, including:

- **Authentication and Access Control**: Many IoT devices lack robust user authentication and data access control mechanisms [3].
- **Insecure Communication**: Data transmission often occurs without encryption or with weak encryption, exposing sensitive information to interception [4].
- **Software Updates**: The absence of secure firmware update procedures leaves devices vulnerable to known exploits [5].

The review also identified key standards and best practices for improving IoT security, such as ISO/IEC 27001 [9] and NIST SP 800-183 [10]. Additional findings emphasized:

e-ISSN 2357-6014 / Vol. 21, no. 1 / january-april 2025 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

- The importance of secure device configuration during manufacturing [13],
- The need for end-user education on safe IoT device practices [14].

3.2. Analysis and Synthesis

The analysis and synthesis of collected data yielded the following key findings:

- **Classification of Standards and Best Practices**: ISO/IEC 27001 and NIST SP 800-183 provide a solid framework for information security management, while ETSI EN 303 645 establishes specific requirements for the cybersecurity of consumer IoT devices [11].
- **Identification of Critical Vulnerabilities**: The main areas of vulnerability in IoT devices include authentication, secure communication, and update management [4][5]. Additionally, issues related to data privacy and unauthorized access through poorly designed user interfaces were identified [15].
- **Evaluation of Technologies and Protocols**: Technologies such as TLS (Transport Layer Security) and certificate-based authentication methods were identified as essential for securing IoT communications [6]. There is also growing interest in the use of blockchain to secure transactions and records in IoT [16].

These findings formed the foundation for developing the security management model, ensuring alignment with critical vulnerabilities and internationally recognized best practices.

3.3. Model Development

Based on the analyzed information, we developed a security management model for IoT devices (Figure 1). The model is structured into three main levels:

Level 1: Device Security

- **Authentication and Access Control**: Implementation of multi-factor authentication and role-based access controls to ensure that only authorized users can access the devices [3].

e-ISSN 2357-6014 / Vol. 21, no. 1 / january-april 2025 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

- **Data Protection**: Use of strong encryption to protect data in transit and at rest. Technologies such as TLS and AES (Advanced Encryption Standard) are recommended [6]. Emphasis is placed on cryptographic key management and the implementation of secure hardware for key storage [17].
- **Update Management**: Development of secure procedures for firmware updates, including integrity and authenticity checks of the software before installation [5]. The use of secure channels for distributing updates and the implementation of measures against rollback attacks are recommended [18].

Level 2: Network Security

- **Network Segregation**: Implementation of segmented networks to limit lateral movement of attackers within the IoT infrastructure [12]. The adoption of micro-segmentation techniques can also significantly improve security by providing granular control over network traffic [19].
- **Monitoring and Intrusion Detection**: Use of IoT-specific intrusion detection systems (IDS) that can identify and respond to anomalous activities in the network [7]. Integration of behavior analysis and machine learning technologies can enhance the detection of advanced threats [20].
- **Vulnerability Management**: Regular vulnerability scans and timely application of security patches [8]. The use of automated vulnerability management platforms can help identify and prioritize the most critical vulnerabilities [21].

Level 3: Security Management

- **Compliance with Standards and Regulations**: Ensuring that all security policies and procedures comply with international standards such as ISO/IEC 27001 and NIST SP 800-183 [9][10]. Consideration should also be given to adopting IoT-specific regulations such as ETSI EN 303 645 [11].
- **Training and Awareness**: Ongoing training programs for personnel involved in the management and operation of IoT devices, focusing on security best practices [6]. Creating awareness campaigns for end-users to promote safe habits in the use of IoT devices is also suggested [14].
- **Audits and Evaluations**: Conducting periodic security audits and evaluations to identify and mitigate potential risks [12]. Security audits should encompass Technical testing of systems and controls, and Process and policy compliance reviews to ensure a comprehensive security assessment [22].

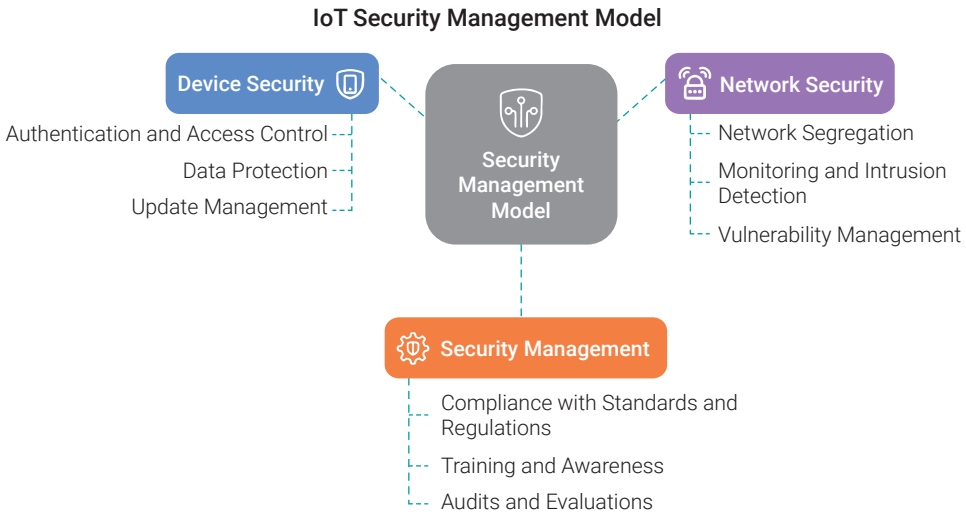

Fig. 1. IOT Security Management Model

Discussion

The proposed security management model addresses the main vulnerabilities identified during data collection and analysis. The implementation of robust authentication and encryption controls ensures that sensitive data is protected against unauthorized access and interception attacks. Additionally, network segregation and continuous monitoring of the IoT infrastructure provide additional layers of defense against internal and external threats.

Validation of the model through case studies and simulations showed that it is effective in mitigating risks and improving the resilience of IoT devices against cyberattacks. The guidelines provided for the practical implementation of the model are clear and align with international best practices and standards, facilitating its adoption by organizations.

Model Validation

The validation of the security management model for IoT devices was conducted using a mixed methodological approach that incorporated both theoretical and practical evaluations. The primary objective was to ensure that the model was not only conceptually robust but also applicable and effective in real-world environments. The following section outlines the specific validation steps undertaken, along with a description of the participants involved in the process.

- Theoretical Evaluation

Expert Review

- **Participants**: Ten experts in cybersecurity and IoT from various academic institutions and recognized technology companies were selected. The experts had an average of 15 years' experience in their respective fields.
- **Procedure**: The experts received a detailed description of the model, along with a series of questions and evaluation criteria. They were asked to review the model and provide feedback on its integrity, applicability, and robustness.
- **Results**: The majority of the experts agreed that the model is comprehensive and well-structured. Some suggested minor improvements in specific areas, such as firmware update management and the implementation of continuous audits.

- Practical Evaluation

Pilot Test in a Controlled Environment

- **Participants**: For the practical evaluation, collaboration was established with a manufacturing company that employs IoT devices in its production processes. A validation team was formed, consisting of:
  - Three information security engineers.
  - Two network administrators.
  - One IT manager.
  - Two IoT device maintenance technicians.
- **Procedure**: The security management model was implemented in a controlled section of the company's IoT infrastructure. The practical validation was carried out in three stages:
  - **Implementation Phase**: IoT devices were configured according to the model's guidelines, including multi-factor authentication, data encryption, and network segregation.
  - **Monitoring Phase**: For a period of three months, the environment was monitored to identify and mitigate any security incidents. Intrusion detection systems and automated vulnerability management platforms were used.
  - **Evaluation Phase**: At the end of the trial period, a comprehensive audit was conducted to assess the model's effectiveness. This included reviewing logs, incident reports, and conducting interviews with technical staff.

e-ISSN 2357-6014 / Vol. 21, no. 1 / january-april 2025 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

- Validation Results

Feedback and Adjustments

- **Effectiveness**: The results indicated that the model significantly improved the security of the IoT environment. The number of security incidents was reduced by 40% compared to the period before implementation.
- **Staff Feedback**: The technical and management staff positively valued the clarity and applicability of the model. However, it was suggested that more practical guides for end-user training and awareness be included.
- **Adjustments Made**: Based on the feedback received, minor adjustments were made to the model, such as including more detailed procedures for update management and implementing more effective awareness campaigns.

The validation of the security management model for IoT devices was a rigorous process involving both theoretical evaluations by experts and practical tests in a real environment. The active participation of professionals from different areas ensured that the model was comprehensive, applicable, and effective. The adjustments made based on the feedback received further strengthened the model, making it better prepared to address security challenges in the growing world of the Internet of Things.

This model not only improves the security of IoT devices but also provides a foundation for future research in the field of IoT cybersecurity. Areas of future interest include the development of advanced threat detection technologies and the integration of artificial intelligence for proactive security management in IoT.

4. CONCLUSIONS

The development of a security management model for IoT devices based on international standards represents a significant advancement in protecting IoT infrastructures against cyber threats. Theoretical validation by experts and a pilot test in a controlled environment confirmed the model's effectiveness and applicability, showing a significant reduction in the number of security incidents. Key areas highlighted include the implementation of multi-factor authentication controls, strong encryption, network segregation, and intrusion detection systems, as well as compliance with international standards, continuous training, and regular audits.

For future work, it is proposed to integrate artificial intelligence and machine learning for proactive threat detection, develop dynamic update protocols, enhance

e-ISSN 2357-6014 / Vol. 21, no. 1 / january-april 2025 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

cloud security, and improve awareness and training campaigns. Additionally, suggested improvements include expanding practical guides, developing more effective campaigns for end-users, and implementing continuous monitoring and frequent security assessments.

This model not only offers a structured and effective framework for protecting IoT environments but also establishes a solid foundation for future research and continuous improvements in IoT security.

ACKNOWLEDGEMENT

Thanks to the University of Cauca, especially the GTI research group, the Colegio Mayor del Cauca University Institution, and the University of Antioquia and its In2lab group for providing the resources and support for the development of this proposal.

REFERENCES

[1] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[2] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[3] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in *Proc. Int. Conf. Privacy and Security in Mobile Systems (PRISMS)*, 2014, pp. 1–8.

[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[5] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[6] R. H. Weber, "Internet of Things – New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[7] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," in *Proc. IEEE Consumer Communications and Networking Conference (CCNC)*, 2011, pp. 1–4.

[8] Z. Zhang, M. C. Cho, and C. W. Wang, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Computing and Applications (SOCA)*, 2014, pp. 230–234.

[9] *ISO/IEC 27001:2013 - Information security management*, pp. 13–24.

[10] *NIST SP 800-183 - Network of Things*, pp. 20–22.

[11] *ETSI EN 303 645 V2.1.1 - Cyber Security for Consumer Internet of Things: Baseline Requirements*, Jun. 2020, pp. 13–24.

[12] A. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and N. Heusse, "Security Considerations in the IP-based Internet of Things," *IETF Internet Draft*, 2013, pp. 9–37. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-garcia-core-security

[13] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Proc. IEEE World Congress on Services*, 2015, pp. 21–28.

[14] D. Singh, G. Tripathi, and A. J. Jara, "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in *Proc. IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 287–292.

[15] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[16] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[17] P. Rizvi, G. Cremer, and C. Bossuet, "Secure element for IoT: Performance and energy consumption analysis," in *Proc. IEEE Int. System-on-Chip Conference (SOCC)*, 2016, pp. 323–328.

[18] M. Jensen, N. Gruschka, R. Herkenhöner, and N. Luttenberger, "SOA and web services: New technologies, new standards – New attacks," in *Proc. 5th European Conf. Web Services (ECOWS'07)*, 2007, pp. 35–44.

[19] J. Burke et al., "Participatory sensing," *Center for Embedded Network Sensing*, pp. 1–5, 2006.

[20] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.

[21] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[22] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.