Computers, Materials & Continua
DOI:10.32604/cmc.2021.014165
Article

Tech Science Press

Security Requirement Management for Cloud-Assisted and Internet of Things—Enabled Smart City

Muhammad Usman Tariq[1], Muhammad Babar[2], Mian Ahmad Jan[3,4,5,*], Akmal Saeed Khattak[6], Mohammad Dahman Alshehri[7] and Abid Yahya[8]

[1]Abu Dhabi School of Management, Abu Dhabi, 6844, United Arab Emirates
[2]Department of Computing and Technology, Iqra University, Islamabad, 44000, Pakistan
[3]Institute of Research and Development, Duy Tan University, Da Nang, 550000, Vietnam
[4]The Faculty of Information Technology, Duy Tan University, Da Nang, 550000, Vietnam
[5]Department of Computer Sciences, Abdul Wali Khan University, Mardan, 23200, Pakistan
[6]Department of Computer Sciences, Quaid-i-Azam University, Islamabad, 44000, Pakistan
[7]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[8]Botswana International University of Science and Technology, Palapye, 016, Botswana
[*]Corresponding Author: Mian Ahmad Jan. Email: mianahmadjan@duytan.edu.vn
Received: 03 September 2020; Accepted: 08 November 2020

Abstract: The world is rapidly changing with the advance of information technology. The expansion of the Internet of Things (IoT) is a huge step in the development of the smart city. The IoT consists of connected devices that transfer information. The IoT architecture permits on-demand services to a public pool of resources. Cloud computing plays a vital role in developing IoT-enabled smart applications. The integration of cloud computing enhances the offering of distributed resources in the smart city. Improper management of security requirements of cloud-assisted IoT systems can bring about risks to availability, security, performance, confidentiality, and privacy. The key reason for cloud- and IoT-enabled smart city application failure is improper security practices at the early stages of development. This article proposes a framework to collect security requirements during the initial development phase of cloud-assisted IoT-enabled smart city applications. Its three-layered architecture includes privacy preserved stakeholder analysis (PPSA), security requirement modeling and validation (SRMV), and secure cloud-assistance (SCA). A case study highlights the applicability and effectiveness of the proposed framework. A hybrid survey enables the identification and evaluation of significant challenges.

Keywords: Security; privacy; smart city; Internet of Things; cloud computing

1 Introduction

The expansion of the Internet of Things (IoT) is a huge step in the development of the smart city [1]. The IoT infrastructure for a smart environment includes devices, objects, sensors, and citizens. The IoT-based smart city ecosystem provides digital traces of activities that can be collected and analyzed [2]. The objective of IoT applications is to efficiently utilize IoT resources. The IoT is favored because it improves peoples' quality of life. Domains and applications of smart environments based on the IoT infrastructure must accommodate a wide range of devices with varied requirements.

Cloud computing comprises storage, software, and shared networks that are available through the internet. Cloud computing is a grid of all resources (e.g., servers and applications) placed in a shared location that can be accessed by a network, service providers, and users who can conveniently pay as they go [3]. A service level agreement (SLA) assures the availability of resources. The IoT started in organizations that prioritize fast communication to minimize network transmission. It is risky to adopt because flaws exist in some applications, including poor management of security requirements [4]. Cloud computing can be useful in smart cities, as it provides easy information sharing, dynamic response, follow-to-stakeholder necessities, and requested load, which demand all the applications included in the smart city.

In the IoT environment, stakeholders are distributed geographically, making it difficult to implement traditional security requirement management. Several proposals highlight that the modification and extension of existing traditional techniques could be helpful, and others relate to novel methods or frameworks. Security is a significant concern in IoT-enabled applications [5,6]. Generally, only functional requirements are considered during requirement management, and maintenance and non-functional requirements are left to be considered in the design and implementation stages. Requirement specification has a significant role in the development process of any system; hence, requirement engineering is significant in dealing with IoT systems.

Security issues should be highlighted in the early stage of development. Various approaches have been introduced to enhance the security of IoT-enabled applications. Traditional methods are insufficient due to problems of inconsistency and scalability. The requirements of the system are systematically collected using requirement engineering (RE) process [7]. Industry focuses on functional requirements, and other requirements are left for the design and implementation phases of development, which results in inconsistency and ambiguity. Requirement engineering used to define the requirements of a system. The quality of the system is based on requirement conformance.

Success in the transformation from traditional system to the IoT depends on the meeting of security requirements, and better requirement engineering leads to a better cloud system [8]. Security requirement engineering is the most significant aspect in the development of IoT-enabled applications [9], and it plays a significant role in the development of cloud-assisted applications. Security requirements in IoT and cloud computing focus on quality attributes such as security, availability, privacy, and accessibility [10]. A smart environment consists of IoT devices that require efficient requirement collection, investigation, and documentation. Well-organized, thorough requirement investigation is not promising through customary techniques. The IoT and the cloud are the two most significant models of ICT that are determining the next generation of smart cities. Both have a notable effect on how we shape and position smart applications for smart cities. The cloud paradigm epitomizes the distribution of software and hardware. Alternatively, the

IoT notion foresees a novel cohort of devices or things that are associated with the internet that supports the smart cities.

Standard practices (such as security requirement management techniques used for classical systems) are mostly incomplete. Few security requirement management techniques other than general techniques (such as the RE framework for cloud-based applications and RE model for real-time applications) are intensively used with limited security feature management. However, no all-inclusive, all-purpose, effective solutions are available to manage security requirements in the cloud and IoT. It is important to recognize the challenges of such applications. A specific security requirement framework is required. This research work studies security requirements of IoT-enabled systems and devises a framework to collect them.

2 Literature Review

We review security requirement management tools, techniques, frameworks, and methods used to collect requirements for IoT-enabled applications in domains such as embedded systems, critical systems, and cloud computing. Various researchers have considered the security requirements of cloud computing in the initial phase of system development. A method was proposed to accumulate security requirements using a game approach [11], which is efficient in the rare case that requirements are specific and known. A model of security requirements for cloud-enabled applications was developed using unified modeling language (UML), which collects requirements for cloud systems [12]. A framework was proposed to gather requirements for clouds that are inaccessible. This framework is more suitable to modifications of requests [13]. Security requirements for cloud service providers were analyzed from the client's perspective by creating client files known as fuzzy Galois lattices [14].

A framework was proposed to develop cloud applications [15]. Security should be involved in the initial stage of developing a software system. Storytelling is a requirement-elicitation technique but cannot be used to elicit cloud requests for cloud-assisted systems. Another framework to collect security requirements for a cloud system lacked the identification of security requirements at an early stage [16]. Security challenges caused the failure of a cloud-assisted system [17,18]. An integrated model provided security in the software development life cycle (SDLC) of cloud applications. The set of techniques was used to practice security management in the cloud [17]. A strategic vision based on engineering principles was proposed to cover the requirements of cloud-assisted applications [18]. A framework was proposed that work in combination with the service development life cycle to prevent the system from failures [19]. This proposal defined techniques for software requirement elicitation, analysis, and modeling. The authors also suggested some future direction regarding software requirement engineering research.

Tariq et al. [20] stressed the need for correct requirement management process, and highlighted the best methods for various types of projects. A field study based on empirical evidence highlighted how remote interaction and differences in culture, time, and language influence security requirements. Elicitation techniques include protocol analysis, document reading, joined application development (JAD) sessions, interviews, video, audio transcripts, observation, uses, and scenarios. An RE process based on exploratory studies and stakeholder exercises was described [21], and requirement engineering approaches specific to home care systems were suggested. Experts interviewed participants from seven companies to obtain their views on RE practices in the embedded systems industry [22]. A field study was conducted based on empirical evidence. The remote interaction between distributed stakeholders in IoT and cloud-assisted applications were

considered, but only a review was provided [23]. We conclude that a standard requirement engineering process is needed for software development.

This study explores security in the context of the IoT and cloud-based systems, and state-of-the-art practices to escalate and optimize RE security. A security requirements management framework is required to face security challenges in cloud-assisted IoT systems. Another goal is to obtain a methodology to manage security requirements in the early stage of software development so that systems are secure.

3 Proposed Framework

We explain the framework of this research work. An IoT-enabled and cloud-assisted smart city is depicted in Fig. 1. Such a city generates information that must be handled securely. Security concerns are forwarded to the cloud for processing.

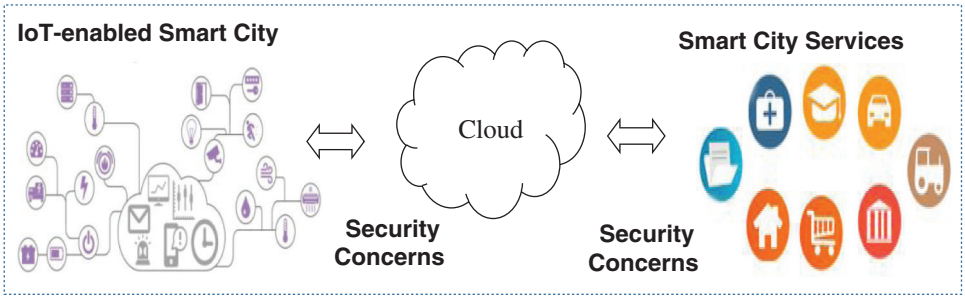

Figure 1: IoT-enabled and cloud-assisted smart city

3.1 System Overview

Fig. 2 depicts the workflow of the proposed framework. Data are generated by IoT devices including environmental sensors, cameras, and reliable stakeholders, and digital systems log these data and check it for anomalies. Proper security requirement management is presented in Fig. 2. Requirement specification and validation are performed on the security requirements of the smart city. The security requirements are forwarded to the cloud for processing and storage. Cloud providers consider security and privacy, and operational management checks security parameters. The guard management process includes two different layers (e.g., manager layer and administrator layer). Finally, decision management is performed using the secure environment.

3.2 Proposed System

The proposed architecture includes modules for stakeholder analysis (PPSA), security requirements modeling and validation (SRMV), and secure cloud-assistance (SCA), as shown in Fig. 3.

Initially, the cloud security requirements are considered for IoT applications by proposing security model. The proposed security management model is compared with state-of-the-art proposals. We suggest methods for security requirement management, such as requirement collection, investigation, documentation, modeling, and validation. The proposed model includes specific methods for cloud-assisted IoT-enabled smart environment. The proposed methods are executed using appropriate configuration setting of IoT and cloud-assisted systems. This model can reduce the development cost and time of IoT-based systems.

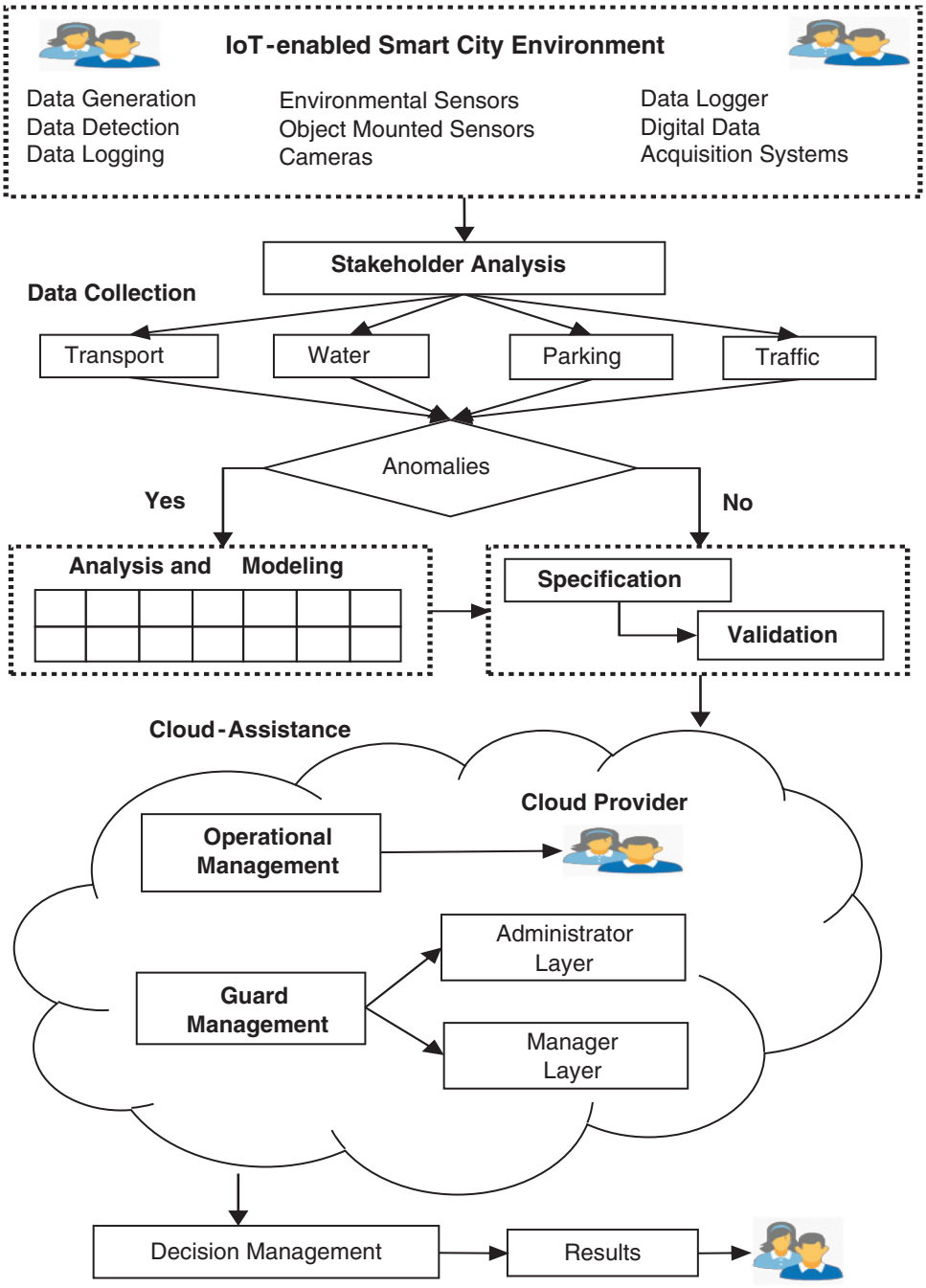

Figure 2: System workflow

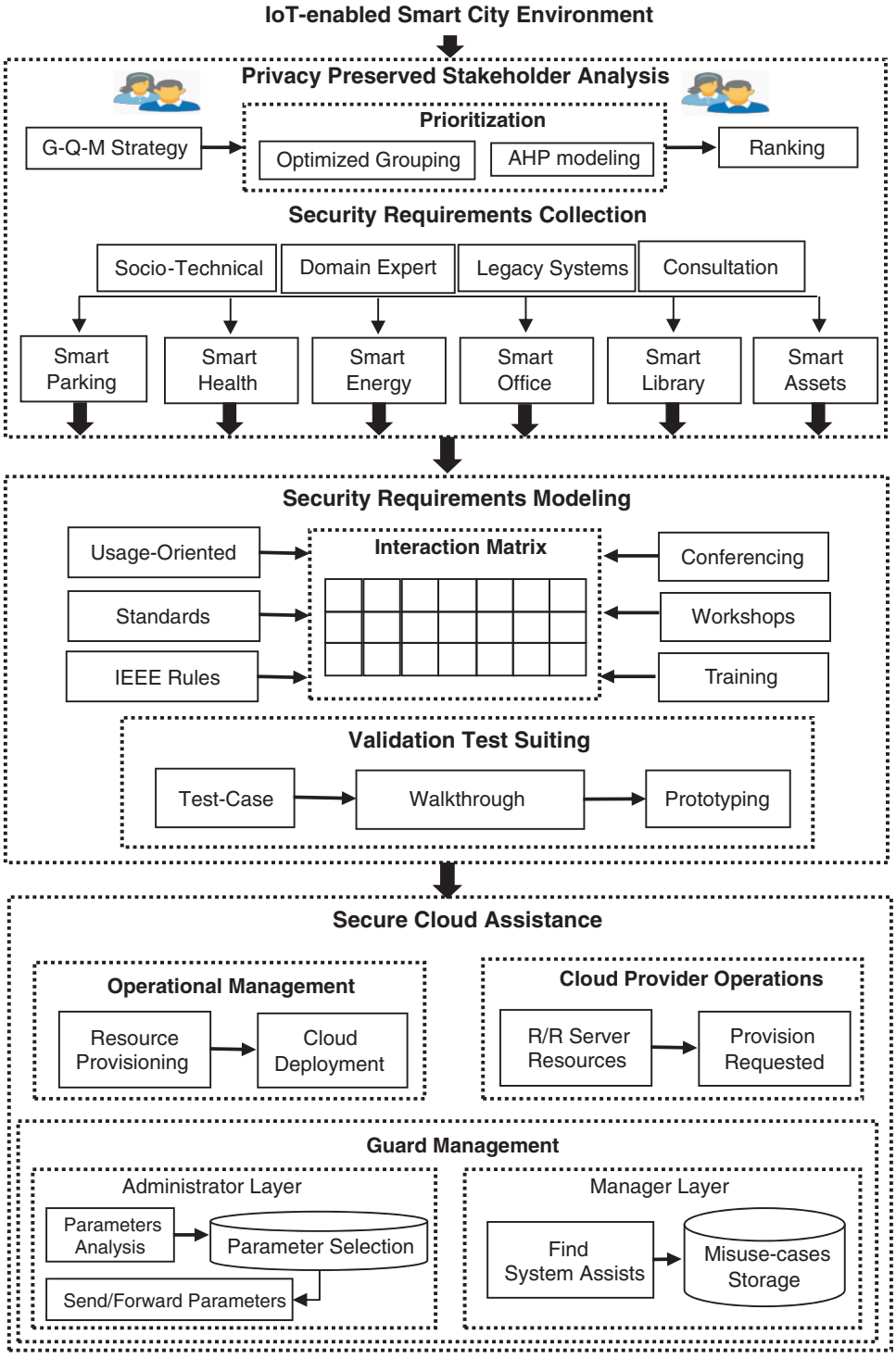

Figure 3: Proposed framework

3.2.1 Privacy Preserved Stakeholder Analysis (PPSA)

We utilize the goal-question-metric (GQM) approach in the PPSA module for stakeholder analysis. Questions are designed to classify stakeholders. The optimized grouping method and analytical hierarchy process (AHP) perform prioritization. The optimized grouping method avoids biased decisions. This approach groups security requirements based on resource availability, importance, and development. Stakeholders are ranked after integrated prioritization. Security requirements are collected using a socio-technical approach, legacy systems, domain expertise, and specific consultation. Stakeholder requirements are captured by experts. The socio technical approach includes the legacy system of IoT, conferencing, and domain analysis with a domain expert's opinion. IoT application stakeholders are available in a distributed manner; hence, Web conferencing is preferred. Domain experts are used for new domains with limited prior knowledge. It is useful to highlight challenges in old systems for application to new systems. Security requirements are grouped, e.g., for parking, health, offices, libraries, and energy.

3.2.2 Security Requirements Modeling and Validation (SRMV)

We integrate the proposed framework with usage-oriented analysis (UOA). It is useful to understand the new system from a usage perspective when the literature is insufficient. Similarly, we suggest interactive workshops along with training on IEEE rules for requirement specification. UOA has a strong association with an interactive matrix in a unified process to document security requirements. The interaction matrix is useful for analysis of the communication gap between stakeholders. A test-driven approach for requirement validation turns requirement into more specific case to check the validity of security requirements for new domains. The requirement analysis is used to analyze the security requirements collected for cloud-assisted IoT applications. Negotiation in this phase eliminates uncertainties. Requirements are specified in a software requirement specification (SRS). The interactive workshops and IEEE rules are integrated; the integration will be a unified process for security requirement documentation.

An interactive workshop involves training to cover IoT needs, and techniques to validate the security requirements of cloud-assisted IoT applications. Workshops can efficiently document security requirements. Requirement validation verifies processes adopted for a particular system. The last step is to validate security requirements for correctness and consistency. Test case generation and prototyping techniques are utilized in the proposed model. We prefer test suiting, which is a test-driven approach to turn requirements into specific cases to check anew domain's validity.

3.2.3 Secure Cloud Assistance (SCA)

The cloud agent's security requirement management is conducted using a secure cloud assistant (SCA), which integrates an i* hierarchy, (security requirements elicitation and assessment mechanism) SecREAM, hierarchical*, and theoretical deception mechanism [24–27]. The i* hierarchy is goal-oriented, SecREAM is asset-based, hierarchical i* is an extension of i*, and the theoretical deception mechanism conceptually describes security requirements. The i* hierarchy has director, manager, and administrator tiers, and actors who perform activities to accomplish goals. The traffic warden and cloud provider are the main actors. The traffic department offers online registration services to citizens. SecREAM is an asset-based ranking methodology that collects application security requirements. We identify the stakeholders using the model's privacy preserved stakeholder analysis (PPSH) mechanism to collect security requirements. Actors play a significant role in hierarchical approaches, and a new actor can help collect security requirements. Hence a privacy preserved stakeholder analysis module is introduced.

We discuss each layer of the hierarchy, where guarding security is the goal of each layer. The operational manager manages the whole process to realize the transportation system's online services. The traffic department manager deploys software within cloud services and IoT-enabled smart services. The cloud provider operator offers cloud resources. A guard at the administrator layer contains a repository for security parameters and issues alerts regarding security issues. The cloud user performs data processing and data storage activities. Finally, the proposed model creates misuse cases for each parameter that expresses the security threats for the smart transportation system. The parameters are stored in the pool or repository by the database administrator. The repository consists of assets of the system with their respective parameters.

4 Results and Discussion

We elaborate on the concept of IoT-enabled smart cities with cloud assistance and validate the proposed framework using a cloud-assisted IoT setting. The traffic system requires a significant upgrade to exploit technological advances, especially in data communication and networks. We designed a survey from the perspective of a stakeholder who is accessing the cloud. It addresses storage and processing. Fig. 3 depicts storage analysis.

Parameter authentication ranks highest in the smart transportation scenario. Similarly, the authorization parameter is ranked second highest, which highlights that access to data is a significant concern. Authentication and authorization allow only specific people to access data. Parameters getting average stakeholder votes are ranked medium. The percentage is computed and compared with other parameters, as shown in Fig. 4. Availability and maintainability are also security concerns. The smart IoT system can provide and maintain services to assist users. The configuration and scalability parameters are the non-functional requirements which represent the security threats.

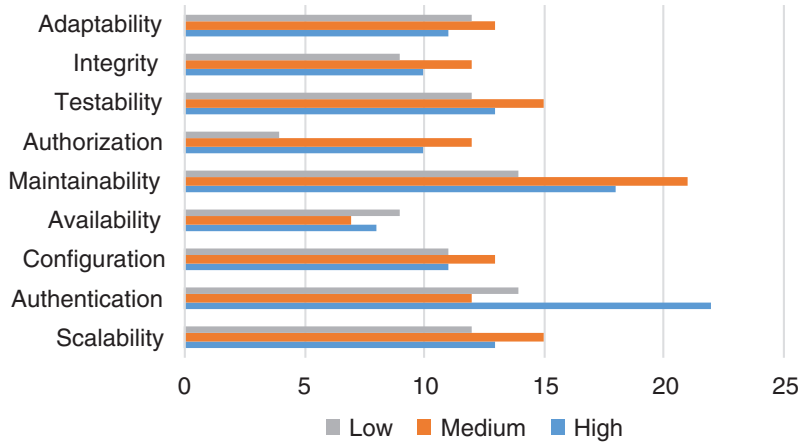

Figure 4: Storage analysis

Fig. 5 shows transaction processing analysis, which is the immediate service of the smart transportation system. The smart IoT system must be available whenever users need it. System downtime should be less than 2 h on work days. The cloud-assisted IoT-enabled smart city system must be maintained at both in bath-processing and real-time processing.

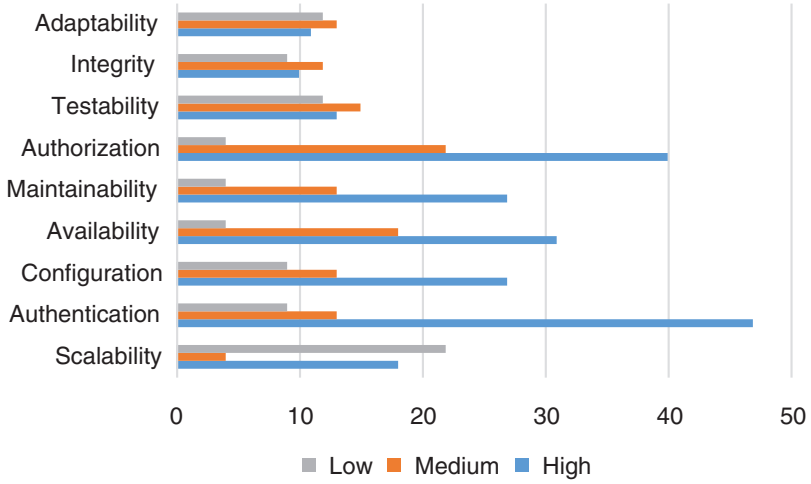

Figure 5: Processing analysis

The second part of the survey concerns data storage and processing. Storage analysis and parameters are shown in Fig. 6. Authentication is significant for the smart transportation system user, as customers are worried about access to this data. The system availability is also significant for the customers as the account holders are related to different domains.

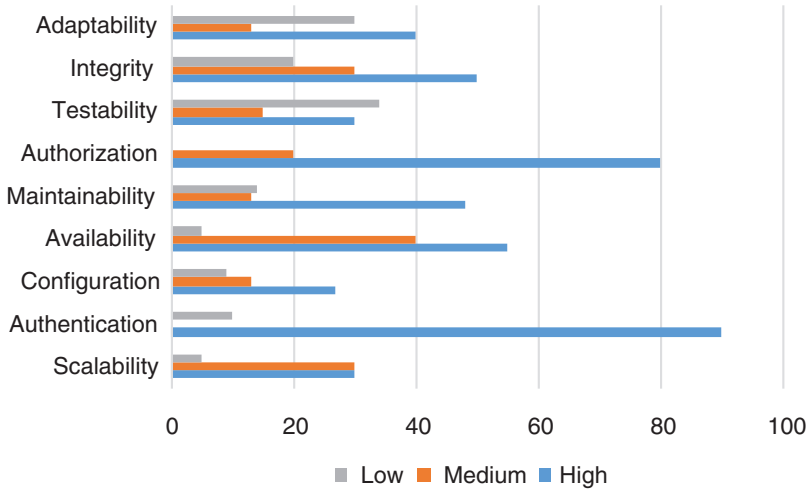

Figure 6: Response of storage analysis

Fig. 7 illustrates transaction processing analysis that is the key service of the smart transportation system. Most citizens are concerned about the storage of their information in a central smart traffic system. They do not permit others to access their data; hence, the authorization score is high. The lower score of integrity indicates that it is of less concern. It is due to the awareness of the integrity parameter in the online system

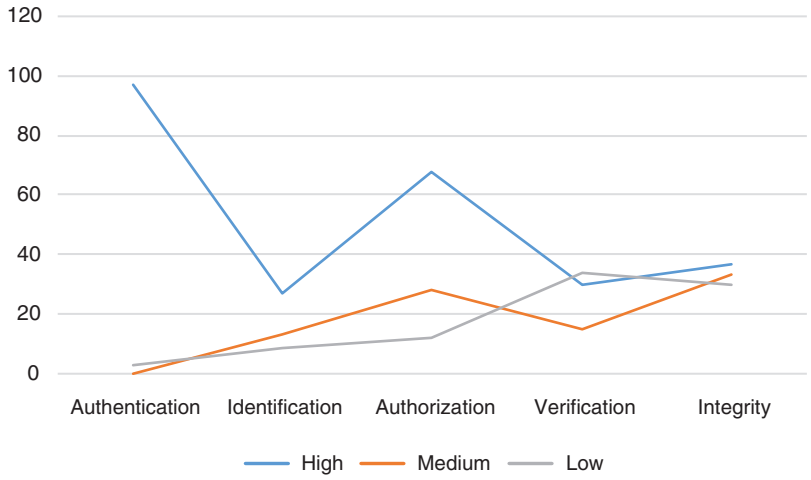

Figure 7: Response to processing analysis

4.1 Comparative Analysis

The proposed framework is compared to existing work to highlight its contributions, considering IoT characteristics as evaluation criteria. We consider the most relevant proposals in the literature that address the specifications of IoT systems. These models provide a high level of abstraction to assess IoT properties during the RE process. We highlight the RE challenges through a hybrid survey. Tab. 1 compares proposals, considering RE challenges as the criteria. Past work has not comprehensively considered these challenges. Wiesner et al. [28] only covered social dissimilarity and challenges of stakeholders during the RE process for IoT. Gonzalez et al. [29] considered IoT understandability and appropriate technique selection for the RE process but overlooked other challenges. Lace et al. [30] covered most RE challenges except social dissimilarity. They described techniques but did not consider practicality and applicability.

Table 1: IoT-enabled systems comparative analysis based on challenges

Challenge	Existing proposals						
	[28] (2014)	[29] (2016)	[30] (2018)	[31] (2015)	[32] (2012)	[33] (2018)	Proposed framework
Domain knowledge management	No	No	Partial	No	Yes	No	Yes
Managing communication gap	No	No	Partial	No	Partial	Yes	Yes
IoT understandability	No	Yes	Partial	Yes	No	Yes	Yes
Dealing with stakeholder challenges	Yes	No	Partial	Yes	Yes	Yes	Yes
Appropriate technique selection	No	Yes	Yes	Partial	Partial	No	Yes
Social dissimilarity management	Yes	No	Partial	No	No	No	Yes

Ksenija et al. [31] dealt with IoT understandability and stakeholder management challenges, and partially covered technique selection. Penzenstadler et al. [32] offered no solution for IoT understandability and social dissimilarity, and partially covered technique selection. Reggio et al. [33] only covered stakeholder management, communication gap management, and IoT understandability. The proposed framework provides solutions to all recognized challenges. We show a comparative analysis of RE activities in Tab. 2, which shows that only Lace et al. [30] covered all activities. However, they did not justify their conceptual solution. Wiesner et al. [28] and Gonzalez et al. [29] only covered the requirement specification. Namirimu et al. [30] only dealt with stakeholder analysis and the elicitation process. Penzenstadler et al. [31] discussed the stakeholder analysis, elicitation process, and requirement analysis, and provided no solution for remaining RE activities. Reggio et al. [32] only covered elicitation and specification activities.

Table 2: IoT-enabled system comparative analysis based on activities

Process activities	Proposals						
	[28] (2014)	[29] (2016)	[30] (2018)	[31] (2015)	[32] (2012)	[33] (2018)	Proposed framework
Stakeholder analysis	No	No	No	Yes	Yes	No	Yes
Information collection	No	No	Partial	Yes	Yes	Yes	Yes
Analysis and modeling	No	No	Partial	No	Yes	No	Yes
Prioritization and negotiation	No	No	Partial	No	No	No	Yes
Requirement specification	Yes	Yes	Partial	No	No	Yes	Yes
Verification and validation	No	No	Partial	No	No	No	Yes

Table 3: Comparative analysis of cloud security requirements

Techniques	P-1	P-2	P-3	P-4	P-5	P-6	P-7	P-8	P-9
[11]	Y	LMT	N	N	N	LMT	Y	Y	N
[12]	N	Y	LMT	Y	Y	Y	N	N	Y
[15]	Y	N	Y	LMT	Y	Y	LMT	LMT	Y
[17]	Y	LMT	Y	N	Y	Y	N	Y	LMT
[18]	Y	Y	LMT	Y	Y	LMT	Y	Y	Y
[25]	Y	Y	Y	N	N	Y	LMT	N	N
[26]	LMT	Y	Y	LMT	Y	Y	N	LMT	LMT
[27]	N	Y	Y	N	N	LMT	Y	N	N
[34]	Y	LMT	Y	N	N	Y	Y	LMT	LMT
[35]	LMT	Y	Y	Y	N	Y	LMT	Y	Y
Proposed	Y	Y	Y	Y	Y	Y	Y	Y	Y

Tab. 3 presents a comparative analysis of security requirement management proposals for the cloud. The first column shows references. The remaining columns compare solutions based on the parameters of P1-scalability, P2-authentication, P3-configuration, P4-availability, P5-maintainability, P6-authorization, P7-testability, P8-integrity, and P9-adaptability. Using the proposed design, a classical method can be customized to collect requirements for cloud-enabled applications, and it relies on how proper requirements (according to IEEE rules) could be collected to design the system. Y, N, and LMT respectively indicate whether a parameter is proposed, is not proposed, or has limited availability. The percentage of threats identified in this study is shown in Fig. 8. Fig. 9 compares the proposed work to existing techniques taking the above parameters into consideration.

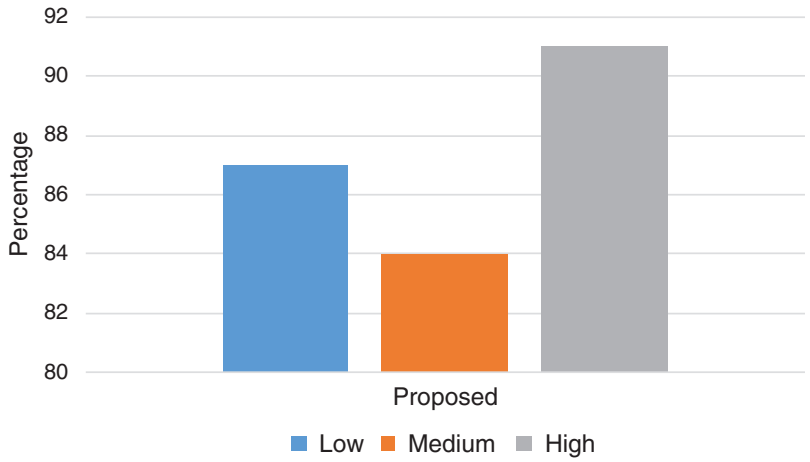

Figure 8: Threat identification ranking position of proposed work

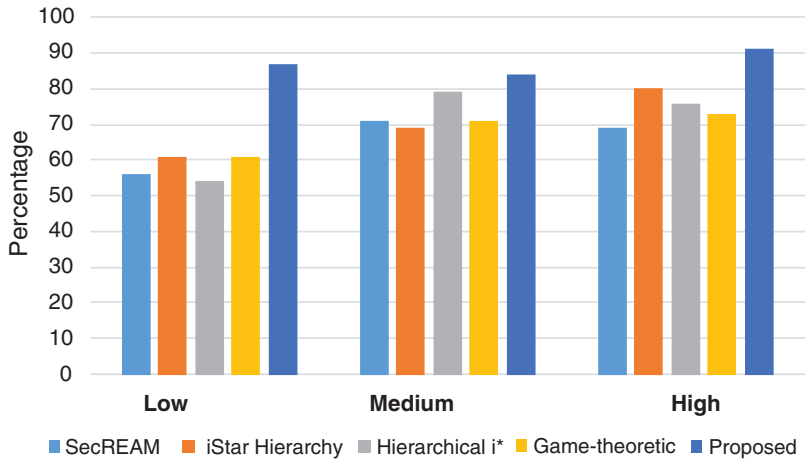

Figure 9: Comparison of proposed work with integrated techniques

5 Conclusion

We proposed a framework to collect security requirements during the early development of cloud-assisted IoT-enabled smart city applications. Security must be considered during initial development. The leading risks of cloud-assisted IoT-enabled smart city environments are availability, security, performance, data confidentiality, and audit and privacy issues. These risks arise due to management of requirements of developing IoT-enabled applications. This work addressed the initial development stage, such as security requirement management. A hybrid survey examined the most demanding requirements of users and associated system security parameters. A case study showed the proposed model's applicability and effectiveness. A comparative analysis of proposed architecture is also provided.

Acknowledgement: Taif University Researchers Supporting Project No. (TURSP-2020/126), Taif University, Taif, Saudi Arabia.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Jeretta Horn, A. Koohang and J. Paliszkiewicz, "The internet of things: Review and theoretical framework," *Expert Systems with Applications*, vol. 133, pp. 97–108, 2019.

[2] M. Yasir, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran *et al.,* "Internet of things based smart cities: Recent advances and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 16–24, 2017.

[3] R. Vanessa, "Cloud computing technology innovation advances: A set of research propositions," in *Disruptive Technology: Concepts, Methodologies, Tools, and Applications*, Hershey, Pennsylvania, USA: IGI Global, pp. 693–703, 2020.

[4] L. N. Bao, E. L. Lydia, M. Elhoseny, I. Pustokhina, D. A. Pustokhin *et al.*, "Privacy preserving block chain technique to achieve secure and reliable sharing of IoT data," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 87–107, 2020.

[5] A. M. Dahman, F. K. Hussain, M. Elkhodr and B. S. Alsinglawi, "A distributed trust management model for the Internet of Things (DTM-IoT)," in *Recent Trends and Advances in Wireless and IoT-Enabled Networks*, Cham: Springer, pp. 1–9, 2019.

[6] A. M. Dahman and F. K. Hussain, "A fuzzy security protocol for trust management in the Internet of Things (Fuzzy-IoT)," *Computing*, vol. 101, no. 7, pp. 791–818, 2019.

[7] A. Naveed and R. Lai, "A method of software requirements specification and validation for global software development," *Requirements Engineering*, vol. 22, no. 2, pp. 191–214, 2017.

[8] Z. Jinxin, Y. Lu, H. Gao, R. Cao, Z. Guo *et al.*, "Comprehensive information security evaluation model based on multi-level decomposition feedback for IoT," *Computers, Materials & Continua*, vol. 65, no. 1, pp. 683–704, 2020.

[9] I. Irum, S. S. Salim, S. Marczak, M. Daneva and S. Shamshirband, "A systematic literature review on agile requirements engineering practices and challenges," *Computers in Human Behavior*, vol. 51, pp. 915–929, 2015.

[10] C. Karl, M. Niazi and J. Verner, "Empirical study of Sommerville and Sawyer's requirements engineering practices," *IET Software*, vol. 3, no. 5, pp. 339–355, 2009.

[11] J. A. Khan, L. Liu, L. Wen and R. Ali, "Crowd intelligence in requirements engineering: Current status and future directions," in *Int. Working Conf. on Requirements Engineering: Foundation for Software Quality*, Amsterdam: Springer, pp. 245–261, 2019.

[12] F. Massimo, F. Palmieri and A. Castiglione, "Modeling security requirements for cloud-based system development," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 8, pp. 2107–2124, 2015.

[13] S. Deepak, C. A. Dhote and M. M. Potey, "Identity and access management as security-as-a-service from clouds," *Procedia Computer Science*, vol. 79, pp. 170–174, 2016.

[14] K. I. Todoran and M. Glinz, "A fuzzy galois lattices approach to requirements elicitation for cloud services," *IEEE Transactions on Services Computing*, vol. 11, no. 5, pp. 768–781, 2015.

[15] A. M. Dahman, F. K. Hussain and O. K. Hussain, "Clustering-driven intelligent trust management methodology for the Internet of Things (CITM-IoT)," *Mobile Networks and Applications*, vol. 23, no. 3, pp. 419–431, 2018.

[16] J. Dhanamma and S. Yeddu, "Cloud SDLC: Cloud software development life cycle," *International Journal of Computer Applications*, vol. 168, no. 8, pp. 6–10, 2017.

[17] R. Muthu, "Software security requirements management as an emerging cloud computing service," *International Journal of Information Management*, vol. 36, no. 4, pp. 580–590, 2016.

[18] A. Shadi, A. Alawneh and R. Jaradat, "Cloud security engineering: Early stages of SDLC," *Future Generation Computer Systems*, vol. 74, pp. 385–392, 2017.

[19] S. Pete, A. Pathak, N. Bencomo and V. Issarny, "How the web of things challenges requirements engineering," in *In. Conf. on Web Engineering*, Berlin, Heidelberg: Springer, pp. 170–175, 2012.

[20] M. Tariq, S. Farhan, H. Tauseef and M. A. Fahiem, "A comparative analysis of elicitation techniques for design of smart requirements using situational characteristics," *International Journal of Multidisciplinary Sciences and Engineering*, vol. 6, no. 8, pp. 30–38, 2015.

[21] M. Lennon and M. Rose, "Requirements engineering for home care technology," in *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, Italy, pp. 1439–1442, 2008.

[22] S. Ernst, B. Tenbergen and K. Pohl, "Requirements engineering for embedded systems: An investigation of industry needs," in *Int. Working Conf. on Requirements Engineering: Foundation for Software Quality*, Berlin, Heidelberg: Springer, pp. 151–165, 2011.

[23] M. Niazi, S. Mahmood, M. Alshayeb, M. R. Riaz, K. Faisal *et al.*, "Challenges of project management in global software development: A client-vendor analysis," *Information and Software Technology*, vol. 80, pp. 1–19, 2016.

[24] O. N. Rizky and K. Surendro, "Requirements engineering for cloud computing in university using i* (iStar) hierarchy method," in *Information Science and Applications*. Berlin, Heidelberg: Springer, pp. 885–890, 2015.

[25] G. Rajat, M. C. Govil and G. Singh, "Security requirements elicitation and assessment mechanism (SecREAM)," in *2015 Int. Conf. on Advances in Computing, Communications and Informatics*, Kochi, India: IEEE, pp. 1862–1866, 2015.

[26] A. Mohammad Taghi, A. Mohammadi, M. H. Manshaei and M. A. Rahman, "A cost-effective security management for clouds: A game-theoretic deception mechanism," in *2017 IFIP/IEEE Sym. on Integrated Network and Service Management (IM)*, Lisbon, Portugal: IEEE, pp. 98–106, 2017.

[27] S. Kridanto and C. Martini, "Hierarchical i* modeling in requirement engineering," *Telkomnika*, vol. 14, no. 2, pp. 784, 2016.

[28] W. Stefan, C. Gorldt, M. Soeken, K. Thoben and R. Drechsler, "Requirements engineering for cyber-physical systems," in *IFIP Int. Conf. on Advances in Production Management Systems*, Berlin, Heidelberg: Springer, pp. 281–288, 2014.

[29] P. Lisardo, G. Tamm and V. Stantchev, "Towards a software engineering approach for cloud and IoT services in healthcare," in *Int. Conf. on Computational Science and Its Applications*, Beijing, China: Springer, pp. 439–452, 2016.

[30] L. Ksenija and M. Kirikova, "Required changes in requirements engineering approaches for socio-cyber-physical systems," in *REFSQ-JP, CEUR-WS*, Netherlands, vol. 75, 2018.

[31] N. Victoria, "User requirements for internet of things (IoT) applications: An observational study," MS. thesis, Faculty of Computing, Karlskrona, Sweden, 2015.

[32] P. Birgit and J. Eckhardt, "A requirements engineering content model for cyber-physical systems," in *Second IEEE Int. Workshop on Requirements Engineering for Systems, Services, and Systems-of-Systems*, Chicago, IL, USA: IEEE, pp. 20–29, 2012.

[33] R. Gianna, "A UML-based proposal for IoT system requirements specification," in *Proc. of the 10th Int. Workshop on Modeling in Software Engineering*, Gothenburg, Sweden, pp. 9–16, 2018.

[34] J. Vijayashree, P. U. Ivy and J. Jayashree, "Requirements elicitation framework for cloud applications," *International Journal of Engineering Research and General Science*, vol. 3, no. 1, pp. 729–733, 2015.

[35] R. Muthu, "Software security requirements management as an emerging cloud computing service," *International Journal of Information Management*, vol. 36, no. 4, pp. 580–590, 2016.