Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI Driven Predictive Cyber-Risk Scoring for IoT Deployments in Smart Cities (Machine Learning for real-time Risk Scoring)

[1]. Salman Khan*, [2]Shahid Mohammed Khan, [3]Mohammed Rasheed, [4]. Saifur Rahman Ansari
1. Application Operations, Siemens - Saudi Telecom Company (STC), Riyadh, Saudi Arabia
2. ICT, Ebttikar Technology Company, Riyadh, Saudi Arabia
3. IT-District Technology Management, KAFD Development & Management Company, Riyadh, Saudi Arabia
4. IT-District Technology Management, KAFD Development & Management Company, Riyadh, Saudi Arabia
**Corresponding Author: salmanmalk7@gmail.com*

ARTICLE INFO

Received: 18 Oct 2024

Revised: 10 Nov 2024

Accepted: 28 Dec 2024

ABSTRACT

The development of Internet of Things (IoT) infrastructures in smart cities has already increased the magnitude, heterogeneity and interconnectedness of urban cyber-physical systems, thus exposing systems to systemic cyber-risk. Conventionally vulnerability-based scoring methods such as fixed severity methods are still inadequate to dynamically changing and large scale IoT ecosystems. The paper introduces a predictive, AI-based structure of cyber-risk scoring that will allow smart cities to scale its risk quantification towards infrastructure levels. The suggested framework combines predicting attack possibilities, situational effects, exposure, asset relevance, and network topology into a unified model of many factors' aggregation. A time-based updating process is proposed to guarantee a controlled risk recalibration when the threat conditions change and a network-aware aggregation policy involves the cascading and systemic propagation of risks in the interconnected IoT infrastructures. In contrast to empirical research in the field of intrusion detection, the study is conceptual and analytical, allowing formalization in mathematics, and theoretical validation, based on scenarios, evaluation. Analytical outcomes reveal that there is a limited scope, proportional responsiveness, temporal consistency, and infrastructure-based distinction of risk representation. The framework also allows policy-controllable prioritization, without reference to particular implementation technologies or datasets. This research will transform current cyber-risk evaluation methods with reactionary metrics that assess individual devices to predictive systemic modeling of risk across networks in smart city existence. The suggested architecture also offers a systematic base to subsequent, practical application, elucidable AI fusion, and operational utilization in next-generation city structures.

Keywords: Smart Cities; Internet of things (IoT); cyber-Risk Scoring; predictive risk modeling, Network-Aware risk aggregation; cybers physical systems; dynamic risk assessment; infrastructure security; AI-based cybersecurity.

1. INTRODUCTION

The swift development of smart cities has resulted in massive implementation of the Internet of Things (IoT) infrastructures in vital urban sphere areas such as transportation, energy, healthcare, water, and security. The IoT-based smart city solutions combine heterogeneous sensors, communication infrastructures, edge computing, and cloud-based analytics to increase operational efficiency and the quality of life. The initial research by Zanella et al. [1] indicated the creation of urban IoT ecosystems as the backbone of the current smart city services and the follow-up research has shown the growing complexity of such infrastructures and the interconnectedness of these infrastructures. Nevertheless, the large connectivity, which makes smart functionality possible, also increases the cyber-attack area. The IoT devices are resource-constrained, heterogeneous and frequently placed in physically-exposed environments, which makes them highly susceptible to exploitation. Roman et al. [2] and Sicari et al. [3] showed that conventional security solutions are not sufficient to deal with the dynamic and distributed aspect of IoT ecosystems. Besides, because of the interdependence of cyber-physical systems, attacks on smart city infrastructures

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

have cascading consequences that increase systemic risk. Traditional cybersecurity risk assessment models, such as matrix-based risk assessment methodologies and vulnerability scoring systems, such as the Common Vulnerability Scoring System (CVSS, are mostly static in nature. CVSS gives standardized measures of vulnerability occurrence in terms of severity of the vulnerabilities, but it fails to dynamically bring contextual aspects like the topology of the network, the importance of assets, or the changing threat intelligence [4]. Likewise, existing risk management models like NIST SP 800-30 [5] offer organized business principles of risk evaluation but would not automatically enable predictive recalibration in real time within resourceful and dynamic IoT settings. Lately, any development in artificial intelligence (AI) and machine learning (ML) has drastically changed the operations of cybersecurity. Intrusion detection, anomaly detection and threat intelligence systems that are run by AI have been shown to be capable of identifying more complex patterns of attack than rule-based systems are [6], [7]. Al-Garadi et al. [8] and Nguyen et al. [9] in their publications address the use of deep learning in contexts related to the Internet of Things to identify distributed attacks and botnet presence. Although these developments have been made, most current research has involved detecting and classifying risks as opposed to incorporating quantification of risks at a system level. There is a major gap hence between AI-driven threat detection concepts and dynamic infrastructure-scale cyber-risk scoring. Although the model used to detect anomalies may be capable of detecting suspicious behavior, they are not always translated into risk scores that are aggregated and are contextualized to help in strategizing the decision-making process in the smart city security operations centers. Also, the infrastructures of smart cities based on IoT are highly interdependent, where failure on high-centrality nodes can spread to other subsystems. In such environments, there is no individual risk but a systemic risk as noted in the studies on cyber-physical security [10]. New studies are underway regarding quantitative and probabilistic methods of cybersecurity risk modeling, such as Bayesian risk networks and attack graph modeling [11], [12]. Such techniques are used to represent probabilistic associations between vulnerabilities and attacks paths but most of the time are not integrated with telemetry and AI developed predictive intelligence in real-time. Besides, most of the available frameworks are either theoretical or specifically oriented to certain areas and not full-fledged smart city ecosystems. Many smart city IoT deployments are dynamic, interrelated, large-scale, which necessitates the need to consider a hybrid framework that combines architectural modeling, predictive intelligence, and mathematical risk aggregation but not be limited to a particular implementation technology. A structure of this sort must be capable of continuing to recalibrate risks, consider propagation effects at the network level and assist in prioritizing at the infrastructure level.

This gap is filled in this paper whereby a layered AI-based predictive cyber-risk scoring architecture is proposed to meet IoT deployments in smart cities. In contrast to the empirical machine learning studies that deal with the model training and performance evaluation, this study takes the conceptual and analytical approach. It also formalizes risk variables, establishes a dynamic updating mechanism and includes network-aware aggregation to assist in quantifying risks at the system level. The framework has been confirmed by both theoretical analysis of scenarios and a comparative analysis of the structure with traditional methods of scoring risk that are fixed.

The main contributions of the work are the following:

- An artificial intelligence-based layered architecture in smart city IoT ecosystems and cyber-risk scoring.
- A multi-factor risk formulation based on mathematically-founded predictive, contextual and network-conscious variables.
- An adaptive recalibration mechanism of risk that relies on a dynamic temporal updating.
- An aggregate model of system-level cyber-risk propagation across interdependent infrastructures.

This study can help to transform the current smart city cybersecurity state of the art to the level of proactive, adaptive, and system-level risk management by connecting the AI-enabled forecasting with the formal assessment of risks and their architectural description.

2. LITERATURE REVIEW

2.1 cities IoT security architectures

Security of smart city infrastructures based on IoT has received extensive research in architectural and protocol viewpoints. Jing et al. [13] conducted a study on security measures at the IoT layers and it is found that heterogeneous

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

device environments need to be safeguarded using adaptive and multi-layered security measures. On the same note, Granjal et al. [14] have offered an extensive review of the IoT communications security protocols, the difficulties associated with authentication, encryption, and resource limitations. Security issues in the context of smart cities are increased due to the combination of cyber and physical systems. In the article by Mohammadi et al. [15], the authors talked about the place of the IoT in large-scale smart city architectures and highlighted vulnerabilities of distributed data processing and edge computing environments. In addition, Conti et al. [16] studied cross-layer attacks in the IoT systems and showed that the vulnerability in one layer can be propagated through communication and application layers. Although the studies offer meaningful architectural insights, they are based mainly on security measures and threat reduction measures, as opposed to dynamic and quantitative frameworks owing to the presence of cyber-risks.

2.2 Quantitative Cyber-Risk Modeling Methods

Assessment of cybersecurity risks has developed out of qualitative matrices into probabilistic and analytical models. Attack graph-based security metrics proposed by Wang et al. [17] was used to calculate the network resilience, which made it possible to model the paths of attacks in a structured way. The study by Poolsappasit et al. [18] proposed dynamic Bayesian networks to manage cybersecurity risks, which included vulnerabilities and threats through probabilistic dependence. Cam [19] pointed out how risk assessment is introduced to the cyberspace-physical systems with special attention to the risk model based on probabilism. These quantitative methods are better than the use of fixed risk matrices, but generally these methods demand pre-defined attack patterns and do not naturally respond to dynamic IoT telemetry. Besides, most probabilistic models are enterprise network-scale and lack explicit support of heterogeneity and scale of smart city IoT ecosystems, comprising thousands of low-power devices alongside high-resiliency infrastructure nodes.

2.3 Cybersecurity AI and Machine Learning

The past years have seen AI and machine learning play a considerable role in cybersecurity operations. Buczak and Guven [20] presented a survey of machine learning methods in detecting cyber intrusions and categorized the approaches as supervised, unsupervised and hybrid methods. Sommer and Paxson [21] critically discussed the drawbacks of machine learning within the context of operational security settings, highlighting the problem of generalization, adversarial manipulation, and implementation. Meidan et al. [22] also used behavioral fingerprinting and machine learning to detect anomalies at the device level in the context of IoT. Besides, Doshi et al. [23] studied the topic of deep learning-based detection of the botnet attacks in IoT networks. These works demonstrate that AI methods can be useful in detecting suspicious activity trends in IoT traffic. Nonetheless, most AI-based cybersecurity studies are centered around the accuracy of detection or classification, or the identification of anomalies. Extremely few studies convert outputs of detection tools into systematic and infrastructure-wide risk quantification systems that can be used in strategic decision-making in smart city security operations.

2.4 Network-Centric and Systemic Perspectives of Risk

In recent studies, focus has been on the fact that cyber-risk of interconnected infrastructures is a systemic and not isolated issue. In their study, Kott and Arnold [24] addressed the notion of networked systems cyber resilience and the authors asserted that centrality of nodes and dependencies on others play a critical role in the vulnerability of the entire system. On the same note, Ganin et al. [25] suggested resilience measures of multi-faceted networks, which demonstrates how cascading failures spread across interconnected infrastructures. The interdependency modeling of cyber-physical systems is very vital in understanding systemic risk. Buldyrev et al. [26] showed the results of cascading disruption caused by failures of interdependent networks. Even though these works offer solid theoretical grounds to network-aware risk analysis, they fail to combine AI predictive elements and real-time recalibration protocols into IoT-driven smart city settings to integrate the synchronized scope and limitations of the representative methods of analyses in the area.To further exemplify how fragmented the existing research streams are, Table 1 encapsulates the breadth and shortcomings of exemplary techniques in the IoT security, quantitative risk modeling, AI-driven predictive detection, and resilience analysis in the scope of the entire context.

Table 1. Comparative Overview of Existing Cybersecurity Approaches in Smart City IoT Context

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Research Domain	Primary Focus	Predictive Capability	Dynamic Updating	Network-Aware Aggregation	Infrastructure-Level Risk Scoring
IoT Security & Architectures	Device protection protocols	Limited	No	Limited	No
Quantitative Risk Models	Probabilistic attack modeling	Partial	Limited	Partial	Limited
AI-based Intrusion Detection	Threat classification	Yes	Yes	No	No
Network Resilience Studies	Cascading failure modeling	No	No	Yes	Partial
Proposed Framework	Integrated risk quantification	Yes	Yes	Yes	Yes

Current solutions, as demonstrated in Table 1, handle individual elements of cybersecurity, but fail to combine predictive intelligence, dynamic updating, and network-based aggregation of this into a single architecture of risk scoring at the infrastructure level. The existence of this structural gap is an incentive to create the suggested hybrid framework.

2.5 Research Gap

The current state of the literature on the IoT security, quantitative risk modeling, and AI-based cybersecurity is rather methodologically disjointed. The research in IoT security is mainly centered on device and protocol hardening, and it does not offer a systematic approach to quantifying risk at the infrastructure level. Quantitative methods like attack graphs and Bayesian structures have probabilistic rigor but are mainly fixed and relying on pre-defined attack patterns; therefore, they are not flexible enough to accommodate the current dynamic Internet of Things analysis. Simultaneously, AI-driven cybersecurity studies are mostly focused on accuracy of detection, as opposed to formalizing the predictive outputs into mathematical-based, multi-factor risk scores. The result of detection is not often converted into system level, dynamically calculated risk scores in consideration of asset criticality and network dependencies. Besides, systemic risk and network resilience research considers the cascading effects of interconnected infrastructures, but does not connect them to AI-based predictive scoring systems specifically designed to address smart city IoT ecosystems.

As a result, there is a real gap in the construction of comprehensive framework that combines predictive intelligence, multi-factor mathematical risk consolidation, temporal dynamic updating, and network-sensitive systemic analysis into the large-scale smart city implementations. This paper will fill this gap by offering an AI-based cyber-risk scoring architecture that connects these two research areas that were formerly disconnected.

3. METHODOLOGY

3.1 Research Design

The given research takes a conceptual and analytic research methodology to create a hybrid AI-based cyber-risk scoring framework of IoT implementations in smart cities. It is not aimed at designing or realising a machine learning model, but specific mathematical formalisation and logical justification is required to construct a precise architectural structure. The study combines system modeling, risk quantification theory and network-based analytical reasoning in order to make cyber-risk assessment dynamic and scalable. There are three big components of the methodological approach namely architectural modeling, formal risk formulation, and theoretical scenario-based validation. This makes sure that the contribution is rigorous but not empirical.

3.2 Approach to Architectural Modeling.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The presented framework is created on the basis of a layered system architecture approach that has been used in cyber-physical infrastructure studies. The IoT ecosystem of smart city is conceptually broken down into functional layers that in combination with each other supply the real-time scoring of risks. This abstraction provides the opportunity to model the data flow, calculate risks, and organize decisions. The architecture is structured into five logical components which are data acquisition, feature extraction, predictive estimation, dynamic risk aggregation and decision support. All the layers have a definite functional purpose as well as they are modular and scalable. The layered modeling method guarantees the interoperability of heterogeneous IoT devices and provides the flexibility to the various domains in the smart city, including transportation, energy, and healthcare. A prototype system or implementation is not built, but the architecture is analytically outlined to show that it is feasible and can be successfully integrated in the current smart city security operations centers.

3.3 Identification and Mathematical Formulation of Risk Variables.

The key risk determinants are defined according to the principles of quantification of cybersecurity and infrastructure risks to allow quantifying cyber-risk in a structured manner. All IoT nodes i are modeled by a set of normalized risk parameters: predicted attack probability P i, impact severity I i, exposure level E i, asset criticality AC i and network influence factor NC i.

The cyber-risk score on the node level is mathematically calculated as.:

$$R_i = w_1 P_i + w_2 I_i + w_3 E_i + w_4 AC_i + w_5 NC_i$$

And w_K denotes weight coefficients such that w_K sums up to 1. This is the multi-factor formulation with a weighted version that makes contextual customisation of the formulations depending on infrastructure sensitivity and policy priorities. It is not confined to any particular machine learning implementation that its formulation is based on, but instead the structural integration of predictive outputs as part of a single risk computation structure.

3.4 Dynamic Risk upgrading mechanism.

A time updating mechanism is presented in order to capture the changing character of cyber threats. Risk score is a time-varying variable and updated by adaptive smoothing formulation.:

$$R_i\,(\mathrm{t}) = \alpha\, R_i\,(\mathrm{t}-1) + (1-\alpha) R_i\,\mathrm{new}$$

where 0<alpha<1 regulates the sensitivity of the system to new threat information or vulnerability information. The given formulation makes risk estimation consistent yet adaptable to the changes in the environment. The dynamic update mechanism makes continuous recalibration to be implemented without model retraining.

3.5 Risk Aggregation at a Network Level.

Since smart city IoT ecosystems are interdependent in nature, the risk of a single device is not assessable in isolation. In order to represent the cascading cyber effects, a system level aggregation model is developed as.:

$$R_{system} = \sum_{i=1}^{N} R_i \cdot \beta_i$$

β_i is the relative power of node iin the network topology. This conceptual influence factor operationally defines connectivity, centrality and propagation potential. The aggregation model offers a global infrastructure-level risk execution and offers system-wide prioritization approaches. The proposed framework is unique as a network-aware formulation, which contrasts with the existing device-level scoring frameworks that are not dynamic. Table 2 presents the functional meaning and systemic contribution of each parameter in a summary to elaborate the role and meaning of each risk determinant employed in the proposed aggregation model.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 2. Risk Variables and Their Functional Roles in the Proposed Framework

Symbol	Variable Name	Functional Interpretation	Contribution to Risk Evaluation
P_i	Predicted Attack Likelihood	Probability of compromise based on predictive intelligence	Enables proactive threat anticipation
I_i	Impact Severity	Potential consequence magnitude if compromised	Reflects operational disruption
E_i	Exposure Level	Degree of external accessibility or vulnerability context	Captures environmental susceptibility
AC_i	Asset Criticality	Importance of node within smart city infrastructure	Prioritizes high-impact components
NC_i)	Network Centrality	Structural influence within IoT topology	Models cascading risk potential

Table 2 shows how the proposed model will incorporate predictive, contextual, and structural factors in one risk quantification system. The asset criticality, as well as network centrality, makes the framework unique compared to antiquated vulnerability-based scoring systems.

3.6 Scenario-Based theoretical validation

In an attempt to determine logical consistency and operational feasibility, the framework is analyzed using a theoretical smart transportation network scenario. The situation takes into account the amplification of vulnerabilities in a gateway node, the further growth of the exposure level, and the wave effects between the associated infrastructure elements. The analytic application of the dynamic risk updating mechanism and the aggregation of the risk at the system-level are used to illustrate the dynamics of the risk scores through time and the decision triggering threshold. It is conceptual and analytical validation. It does not use any dataset, simulated environment, or experimental benchmarking. The aim of this exercise is to show structural coherence, scalability, and applicability of the framework to the real world smart city situations.

3.7 Comparative Analytical Evaluation

Comparative analytical evaluation was done to determine the level of organizational commitment, emotional support, compensation and high turnover rates within the sample population of the study. It is analytically compared to the traditional risk scoring mechanisms which are vulnerability-based scoring and matrix-based risk assessment. The comparison is centered on structural capabilities such as dynamic adaptability, network awareness, predictive integration as well as system level aggregation. This qualitative assessment demonstrates the architectural and methodological innovations of the suggested structure and does not use empirical performance indicators.

4. FINDINGS: ANALYTICAL ASSESSMENT AND HYPOTHETICAL FINDINGS.

4.1 Structural validation of the Framework.

The proposed layered architecture was analytically studied to understand its structural consistence, scalability and logical consistency in large-scale smart city IoT settings. The hierarchy of data acquisition, feature abstraction, predictive estimation, risk aggregation, and orchestration layers provides the modularity of functions without losing the ability to integrate end-to-end. Separating predictive estimation and risk aggregation systems point of view, it ensures that there is architectural flexibility. The predictive part may be replaced or improved without any changes to the mathematical form of the risk computation engine. This proves the fact that the framework is implementation-neutral and flexible to the heterogeneous domains of smart cities. The weighted multi-factor risk formulation is bound and it can be interpreted. The output score of the risk is held constant within a predefined range because all the input variables are normalized and added to each other with the sum of weights being one. This property allows the amplification to be controlled as well as aiding with the consistence of decision threshold calibration.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4.2 Analytical Behavior of Risk Formulation

The mathematical formulation was tested with different parameter settings. When the likelihood of attack rises and other factors being held constant, the overall node-level risk score rises in direct ratio to its weight. It shows linear responsiveness and predictability when exposed to individual threat escalation conditions. In cases where a particular node has a high-asset criticality the formulation focuses on high-impact infrastructure components despite moderate levels of vulnerability. This validates the fact that the model is not limited to technical severity but it takes into consideration contextual significance, which is imperative in smart city implementations. Risk distribution is additional altered by the inclusion of factors of network influence. The more the nodes have high connectivity coefficients, the greater the contribution they make to the risk aggregation at the system level. This is to make sure that the central gateways or key hubs are proportionately given more attention during aggregated risk computations. In general, the formulation is monotonic, bounded, and sensitive consistent, which are desirable quantitative risk modeling characteristics.

4.3 Social Stability Analysis in Time.

To identify the adaptability and stability properties, the temporal updating mechanism was analytically assessed. The degree of the smoothing of the historical value-timeliness trade- off is dictated by the smoothing parameter. In cases where the smoothing coefficient goes close to unity, the system focuses on the historical risk states minimizing sudden volatility that is a result of temporary anomalies. On the other hand, when the coefficient is very close to zero, then there is a high sensitivity to new threat intelligence in the system. This adjustable facility permits policy-based settings relying upon operating priorities. The recursive formulation is such that it converges gradually to new equilibrium conditions in case persistent changes take place in the likelihood of threat or the levels of exposure to the threat. Oscillatory instability is avoided and with recalibration at real-time. This dynamism is especially significant in the IoT ecosystems in which the threats conditions change regularly. In order to demonstrate how the choice of the smoothing affects the dynamic risk evolution, in Figure 1 simulated node-level dynamic risk evolutions are shown in discrete time between three smoothing settings (0.9, 0.5, and 0.2). The simulation presupposes the abrupt rise of the new risk indicator 0 to 0.8 at the time step t=5 in the form of a disclosure of a vulnerability or a high probability of the threat.

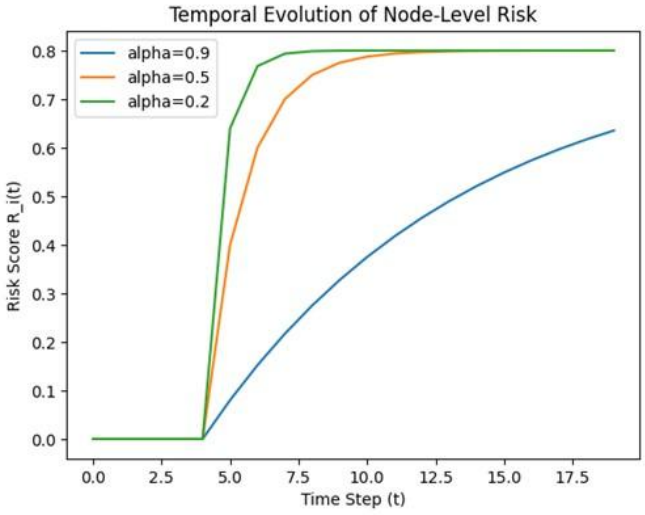

Figure 1. Temporal Evolution of Node-Level Risk Under Different Smoothing Coefficients

Figure 1 indicates that the risk score increases slowly with a value of 0.9; however, when the time step reaches 19, the risk score is about 0.63. This implies a high level of historical inertia whereby the previous risk conditions prevail in the update process. With 0.5 the risk score will approach the new equilibrium value of 0.8 much faster and will have approached it almost, reaching 0.84 by time step 12. The system is very responsive to new threat input when alpha=0.2, and in a few time steps, the system is driven to near 0.8. The following numerical plots prove that the framework offers adjustable responsiveness. Greater values of smoothing encourage resilience, whereas lesser values

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

encourage quick adjustment to arising danger. This ascertains that temporal recalibration is controlled and predictable in relation to adjustments in policy settings.

4.4 Aggregation at the Network-Level and Propagation of Systemic Risk

The system level aggregation model was analytically evaluated to find its capability to reflect interdependences among IoT infrastructures. The aggregated risk, which has been introduced by considering the node influence coefficients, is a measure of both individual vulnerability and structural significance. The score at system level marginally goes up in cases where the risk associated with a peripheral device is high. But, as a high-centrality node of the network, which is the gateway node, is exposed to a high risk, the score at the infrastructure-level goes way up. This shows that this model is successful in differentiating between local and system threats. The analytical aggregation proves the validity of the fact that the cascading cyber effects may be modeled without explicit attack graph simulation. The model makes a shift to a device-based scoring to infrastructure-conscious quantification; this is in line with the systemic character of smart city cyber risk. In order to examine the impact of structural positioning on the IoT topology, Figure 2 demonstrates the correlation between node centrality (between 0.1 and 1.0) and the amount of risk it contributes to the aggregated system-level risk. In this analysis example, the structural risk at the base node is set at 0.6 and centrality values are normalized structural influence in the network.

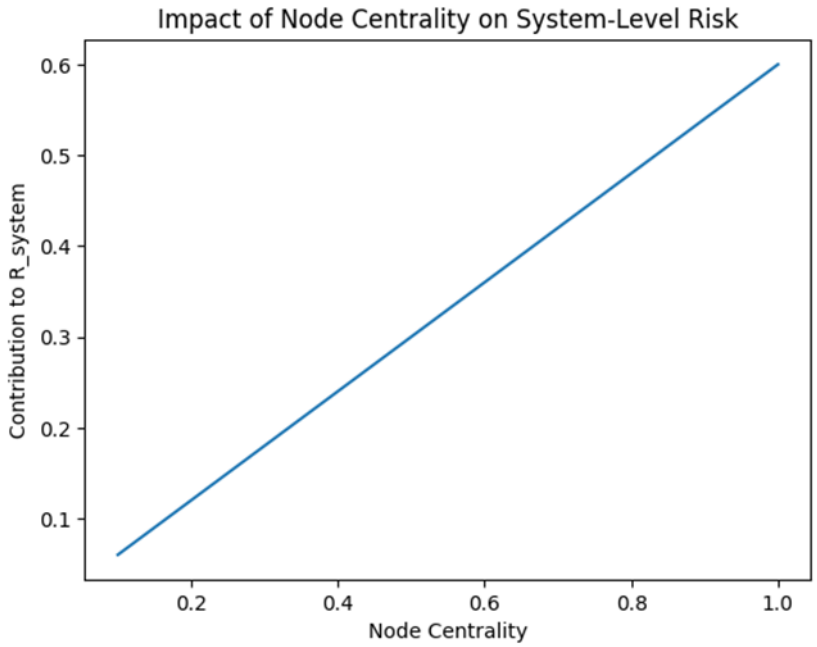

Figure 2. Impact of Node Centrality on Aggregated System-Level Risk

Figure 2 shows that the risk contribution to the system level is proportional to the centrality of the node. As an illustration, a node with centrality of 0.1 is adding about 0.06 to the total system risk, but a node with centrality 1.0 will add 0.6. This quantitative correlation attests to the fact that structurally influential nodes increase the risk on the infrastructure level despite the fact that the risk level of these nodes is equal to that of peripheral nodes. The framework hence rationalizes the distinction of both localized vulnerability with systemic exposure hence making its appropriateness to large-scale smart city environment where the gateway and hub node is significant.

4.5 Hypothetical Smart City Scenarios Evaluation

The framework was tested in a theoretical smart transportation network to prove the practical applicability in a set-up of distributed sensors, intermediate gateways and centralized control units. In the analyzed scenario, there was a vulnerability disclosure that was related to a gateway node and led to an increase in the forecasted attack probability and score. This resulted in a proportional increase in the node-level risk and since the node had high network influence factor, the accumulating system risk also experienced a proportional increase. The temporal update process

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

prevented sharp escalation between time periods and instead of it a gradual recalibration. This analytical development shows that the suggested framework can conceptually model escalation of risks, situational prioritization and systemic amplification in interrelated infrastructures. The situation is authenticated to be operationally viable without empirical simulation.

4.6 Comparative Structural Assessment

There are structural improvements identified when a qualitative comparison is made to traditional vulnerability-based scoring approaches. Traditional scoring systems offer a fixed severity of the score, but they do not incorporate dynamically changing with time, weighted by the dynamic context of the asset, and aggregated by the network sense. Conversely, the proposed architecture merges predictive likelihood estimation, evaluation of contextual impacts, exposure dynamics and systemic propagation into a single model formulated with mathematical terms. Through this integration, infrastructure-level prioritization is possible, as opposed to the isolation of vulnerabilities recorded. The analytical assessment proves the fact that the framework covers the main structural constraints of the existing methods and is also scalable and flexible to the heterogeneous smart city setting. In order to line up the analytical results, Table 3 condences the structural characteristics that were supported in this paper and compares them with conventional and conventional techniques of scoring vulnerability based on its traditional scoring strategy.

Table 3. Structural Evaluation of the Proposed Framework Based on Analytical Validation

Evaluation Criterion	Traditional Vulnerability Scoring	Proposed Framework	Analytical Finding
Risk Adaptability	Static severity values	Time-dependent recalibration	Demonstrates controlled temporal responsiveness
Context Awareness	Limited to vulnerability metrics	Integrates impact, exposure, and asset importance	Enables differentiated infrastructure prioritization
Network Sensitivity	Device-level isolation	Incorporates structural influence factors	Captures systemic and cascading risk potential
Predictive Integration	Reactive assessment	Incorporates predicted likelihood	Supports proactive risk anticipation
Infrastructure-Level Aggregation	Not supported	System-wide aggregation mechanism	Enables holistic smart city risk visibility
Stability Under Variation	May fluctuate with reassessment	Smoothed temporal adjustment	Maintains bounded and stable risk evolution

The analytical assessment as recapped in Table 3 confirms the fact that the proposed framework goes a notch higher than the more traditional vulnerability-based methodology, to the extent that it fosters the capability to quantify the cyber-risk issues on an adaptive, contextual, and infrastructure level. Results show that predictive estimation (augmented), structural influence modeling (augmented) combined with temporal recalibration is a scalable and theoretically consistent mechanism that can be applied to large-scale smart city IoT settings.

5. DISCUSSION

The critical analysis of the suggested framework shows that cyber-threat in smart city IoT settings can be designed as an adaptive, system-wide quantification issue as opposed to a fixed vulnerability listing exercise. The results indicate that the framework is logically consistent across the different threat scenarios and facilitates the prioritization of the infrastructure components differentiated. Among the major findings of this research is the fact that risk responsiveness is predictable and proportional in response to a parameter change. The likelihood of the

attack raises the risk of the node in a predictable and understandable way. Likewise, in the case of high asset criticality, the framework will automatically focus on the high-impact infrastructure nodes. This proves that the model promotes the use of contextual decisions as opposed to technically based severity actions. The updating mechanism dynamically proves to be stable with time as well. The analytical evaluation shows that risk recalibration is gradual as opposed to sudden and thus avoids volatility due to short term anomalies. This feature becomes especially important in smart city infrastructures where the stream of telemetry information flows continuously, and the threat conditions are changing at a high pace. The framework gives hence a responsiveness and stable operations dependency. The other significant conclusion is the paradigm shift of device-centric to infrastructure-level risk representation. The network influence aggregation which is considered at the system level demonstrates that the risks of high-centrality nodes have higher systemic impact than the peripheral devices. This confirms that the conceptualization of cascading cyber-risk potential in the framework is conceptually captivated, despite the absence of explicit attack-graph simulation. Consequently, the infrastructure operators will be able to focus more on mitigation strategies not only on the basis of the severity of vulnerability of the vulnerability but also on the basis of structural significance. The conceptual smart transportation environment also justifies feasibility in practice. The framework conceptually modelled the vulnerability escalation, the situation-specific prioritization, and risk amplification on an infrastructure-wide scale in a coherent way. The node-level escalation and system-level aggregation interaction provides an example of how the threat in localized areas can affect the general risk posture of the urban infrastructure.

Altogether, the results show that predictive likelihood, contextual impact, exposure dynamics, and structural influence can be combined in one aggregation structure to achieve adaptively and scalably scored cyber-risk. The proposed framework, unlike the traditional static scoring system, offers a continuous risk representation with infrastructure awareness that can be used in the environment of smart cities. In a larger sense, this paper runs the conceptual shift of the reactive detection-based security to proactive risk governance. The arrangement of risk as an actively recalibrated and network-conscious entity provides strategic prioritization and policy-tuned adjustment like network-aware tuning, without relying on particular implementation technologies.

In general, the results of the analytical work prove that the offered architecture is conceptually consistent, scalable, and corresponds to the needs of giant IoT-enabled smart cities.

6. CONCLUSION

The proposed study overcame the structural constraints of current methodologies of assessing cyber-risks within smart city IoT by presenting a stratified AI-based predictive cyber-risk scoring model. In contrast to the traditional vulnerability-based approaches based on static measures of severity, the suggested framework combines the predictive likelihood estimation, contextual impact evaluation, exposure dynamics, asset criticality, and network structural impact into a single multi-factor aggregation model. The analytical assessment proved that the framework is bound, proportionate responsive and time stable to diverse threat scenarios. Adoption of a smoothing-based updating mechanism that allows dynamic recalibration of risk scores is not highly volatile and thus, the framework can be applied to dynamic IoT conditions, where telemetry occurs incessantly and attacker surfaces change continuously.

More so, the addition of network influence factors enables the shift in the isolated device-level scoring to the infrastructure-level systemic risk provision. The presented theoretical scenario of smart transportation demonstrated the manner in which the localized increase in vulnerability can be propagated by the means of structural dependencies and affect at the level of the overall system-wide risk. This establishes that the suggested methodology conceptually version captures cascading cyber impacts without taking into account computationally intense attack graph computations. This study will result in the development of cyber-risk models that build upon current paradigms of reactive detection to the formation of adaptive and infrastructure-centric risk governance, by means of connectivity between predictive intelligence and a mathematicalization of risk, and network-aware aggregation. The framework is implementation-agnostic, scalable, and applicable across various spheres of smart cities, thus offering a systematic base of the next-generation approaches to cyber-risk management.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7. FUTURE RESEARCH DIRECTIONS

Although this work has already provided a theoretical and architectural basis, various possible extensions of research are possible. First, quantitative evaluation of predictive accuracy, computation efficiency, and scalability would be empirically validated using real-world datasets of Internet of Things and implemented using a prototype. The combination of the framework and the operational smart city security operations centers can further assess the feasibility of deployment in real-time. Second, explainable artificial intelligence methodology is another research field of interest. The interpretability mechanisms will be necessary to ensure that the policy-level decision-making and regulatory compliance are facilitated by predictive likelihood estimation incorporated into the infrastructure-level risk scoring. Third, the use of federated or distributed learning paradigms could be used to improve privacy-preserving risk estimation, across geographically dispersed subsystems of smart cities. These extensions would enable risk intelligence sharing without having a central data aggregation. Fourth, the future work can be expanded by the aggregation model to nonlinear propagation, or stochastic network modeling to enable cascading cyber-physical interactions to be more fully represented. Last but not the least, the zero-trust principles of architecture and the mechanisms of adaptive scoring of the trust might enhance the resilience to the challenge of insider threats and manipulation of predictive models by adversaries. Together these guidelines offer a channel between the version of concept modeling and operational, scalable, and understandable cyber-incident governance in the next-generation smart urban settings.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.
[2] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.
[3] 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.
[4] FIRST (Forum of Incident Response and Security Teams), "Common Vulnerability Scoring System (CVSS) v3.1 Specification Document," 2019.
[5] National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Rev. 1, 2012.
[6] S. Dua and X. Du, *Data Mining and Machine Learning in Cybersecurity*. CRC Press, 2011.
[7] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.
[8] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.
[9] T. T. Nguyen and G. Armitage, "A Survey of Techniques for Internet Traffic Classification using Machine Learning," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 56–76, 2008.
[10] A. Cardenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems," *ACM Workshop on Cyber-Physical Systems Security*, 2008.
[11] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, Graph-Based Network Vulnerability Analysis," *ACM Conference on Computer and Communications Security (CCS)*, 2002.
[12] Y. Liu and H. Man, "Network Vulnerability Assessment Using Bayesian Networks," *Proceedings of SPIE Defense and Security Symposium*, 2005.
[13] 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.
[14] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.
[15] M. Mohammadi, A. Al-Fuqaha, M. Guizani, and J. Oh, "Semisupervised Deep Reinforcement Learning in Support of IoT and Smart City Services," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 624–635, 2018.

[16] 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.
[17] L. Wang, A. Singhal, and S. Jajodia, "Measuring the Overall Security of Network Configurations Using Attack Graphs," *Data and Applications Security and Privacy*, Springer, 2007.
[18] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, 2012.
[19] H. Cam, "Risk-Based Security Assessment of Cyber-Physical Systems," *IEEE Systems Journal*, vol. 11, no. 1, pp. 238–247, 2017.
[20] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
[21] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," *IEEE Symposium on Security and Privacy*, 2010.
[22] Y. Meidan et al., "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," *arXiv preprint arXiv:1709.04647*, 2017.
[23] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," *IEEE Security and Privacy Workshops (SPW)*, 2018.
[24] A. Kott and C. Arnold, "The Promises and Challenges of Continuous Monitoring and Risk Scoring," *IEEE Security & Privacy*, vol. 11, no. 1, pp. 90–93, 2013.
[25] A. A. Ganin et al., "Resilience and Efficiency in Transportation Networks," *Science Advances*, vol. 3, no. 12, 2017.
[26] S. V. Buldyrev et al., "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, 2010.