

Article

Not peer-reviewed version

Climate Risks to IoT Devices in Kazakhstan: Projections and Adaptation Strategies

[Dinara Zhunissova](#) , [David Topping](#) ^{*} , [James Evans](#) ^{*}

Posted Date: 5 September 2025

doi: 10.20944/preprints202509.0466.v1

Keywords: climate resilience; internet of things; climate change; sensors; cameras; resilient devices; climate modelling



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

Climate Risks to IoT Devices in Kazakhstan: Projections and Adaptation Strategies

Dinara Zhunissova ¹, David Topping ^{2,*} and James Evans ^{3,*}

¹ School of Natural Sciences, Department of Earth and Environmental Sciences, The University of Manchester, Manchester, United Kingdom

² Centre for Atmospheric Science, The University of Manchester, Manchester, United Kingdom

³ School of Environment and Development, The University of Manchester, Manchester, United Kingdom

* Correspondence: david.topping@manchester.ac.uk (D.T.); james.z.evans@manchester.ac.uk (J.E.)

Abstract

This study investigates the vulnerability of Internet of Things (IoT) devices to climate change in Kazakhstan, where extreme seasonal variability and rising climate risks threaten device reliability. Using high-resolution climate projection data from ERA5 and CMIP6 models (RCP4.5 and RCP8.5 scenarios), combined with qualitative interviews with stakeholders in agriculture, energy, transport, and urban infrastructure, we develop risk assessment models for IoT systems. The analysis quantifies device failure probabilities through temperature and humidity thresholds and extends risk curves to include additional climatic stressors such as solar radiation, wind, and snowfall. Results reveal that IoT devices face heightened risks in northern regions during extreme cold events (below -40°C) and in southern regions during prolonged heatwaves (above $+40^{\circ}\text{C}$). Interviews confirm that maintenance, power supply reliability, and device calibration remain major concerns under harsh climate conditions. The findings provide evidence-based recommendations for adaptation strategies, including resilient hardware design, predictive maintenance protocols, and climate-informed deployment planning. This research contributes to the emerging field of climate-resilient IoT, offering both methodological advances and practical insights for policymakers and infrastructure planners in Central Asia.

Keywords: climate resilience; internet of things; climate change; sensors; cameras; resilient devices; climate modelling

1. Introduction

The Internet of Things (IoT) is a transformative technology that connects networked devices capable of collecting and exchanging data, enabling real-time monitoring and control across all industries. IoT is being applied in agriculture, healthcare, energy and urban infrastructure, offering efficiency improvements and automation on a global scale (Atzori et al., 2010a) (Xu et al., 2014), there are several types of outdoor IoT devices, such as cameras, sensors, routers, actuators, Pos terminals and Sim cards, which are widely used in sectors such as agriculture, transport and infrastructure. These devices are crucial for real-time monitoring but are vulnerable to extreme weather conditions. Their importance is emphasised in this research paper on the ability of IoT devices to withstand weather threats and prevent failures in harsh conditions. By connecting devices to central systems, IoT enables data-driven decision-making and has the potential to revolutionise sectors that rely heavily on environmental monitoring and resource optimisation. In Kazakhstan, a country known for its vast territory, diverse topography and extreme weather conditions, IoT systems play a critical role in monitoring environmental parameters, managing urban infrastructure, optimising agricultural activities and energy consumption (Pandiyani et al., 2024, Kazhydromet.kz, 2023).

However, the reliability and sustainability of these IoT systems face significant challenges in the context of climate change, especially in regions with extreme weather conditions. Kazakhstan's

climate is characterised by strong seasonal and regional temperature fluctuations: temperatures can drop to $-44\text{ }^{\circ}\text{C}$ in the northern regions in winter and reach $+45\text{ }^{\circ}\text{C}$ in the southern desert regions in summer (World Bank, 2021). Such extreme temperature ranges can pose operational risks for IoT devices as most of them, such as sensors, cameras, actuators, routers and SIM cards, are designed for certain acceptable environmental conditions. Constant exposure to prolonged summer heat, winter frost and unpredictable temperature fluctuations can lead to device malfunctions, inaccurate sensors and shortened device lifetimes, jeopardising the reliability of these critical systems (Rahmani et al., 2023). In arid and desert climates, overheating and dust accumulation have been identified as key risks for sensor reliability (Algarni and Nutter, 2015).

Climate projections for Kazakhstan indicate not only an increase in average temperatures, but also an increase in the frequency of extreme events, including increased heat waves in summer, severe cold in winter, and unpredictable seasonal transitions. These predictions highlight the urgent need to consider how IoT systems will be able to withstand these conditions. Without proper adaptation, IoT infrastructure can fail anywhere, disrupting critical functions such as agricultural monitoring, power grid management, and urban traffic management (Othmane Friha, 2021). This potential vulnerability emphasises the need for a robust climate risk assessment for IoT infrastructure in Kazakhstan.

This paper addresses the need to quantify climate risks for IoT devices by developing risk assessment curves and climate risk models. While IoT technologies offer promising solutions to improve efficiency and automation, their resilience to climate extremes - especially in vulnerable and unstable regions such as Kazakhstan - is still poorly understood. A deep understanding of climate impacts on IoT systems is critical to building a robust infrastructure that can withstand expected climate stresses, ensuring the efficiency and durability of IoT-enabled services in Kazakhstan.

The Representative Concentration Pathways (RCPs) are widely used climate models developed by the Intergovernmental Panel on Climate Change (IPCC) to represent different greenhouse gas concentration pathways and their potential impacts on global climate (IPCC, 2021). These pathways range from RCP2.6, which involves high mitigation efforts and low greenhouse gas emissions, to RCP8.5, a scenario with high emissions and minimal mitigation. These pathways are important for understanding future climate projections and developing adaptation strategies such as resilience of Internet of Things (IoT) devices.

This study considers RCP4.5 and RCP8.5 scenarios with medium and high emissions. These scenarios are particularly relevant for Kazakhstan and the Central Asia region, as they contain projections of changes in temperature and precipitation that may affect the functionality and resilience of IoT systems. Climate projections derived from these scenarios are the basis for assessing potential environmental risks and planning necessary adjustments to IoT infrastructure.

To model these risks, we used the historical climate data from the Climate Data Store, in particular monthly average ERA5 data (from 1940 to present) and monthly average land ERA5 data (from 1950 to present). Using this data, we developed the risk curves based on the failure rate of IoT devices as a function of temperature deviation from the normal range. These risk assessments will help identify critical thresholds at which the performance of IoT devices may degrade or fail, enabling the development of adaptation strategies that support the resilience of IoT systems in the face of climate variability (Copernicus Climate and Service, 2021). By establishing these thresholds, the study provides recommendations for adaptation measures and resilience planning necessary to ensure the continuity and functionality of IoT systems under future climate projections.

Section 2.

2.1. Global and Regional Perspectives on IoT Resilience to Climate Risks

This section provides an overview of key areas of research on climate risks to IoT systems, measures to increase the resilience of IoT devices in extreme climatic conditions, and specific challenges associated with IoT deployment in Kazakhstan. These studies serve as a basis for

understanding the specific climate vulnerability of IoT devices and identifying necessary adaptation measures.

Globally, IoT systems are increasingly exposed to climate risks such as extreme heat, storms, and humidity fluctuations. Studies in Europe, North America, and arid regions demonstrate that IoT devices are vulnerable when environmental conditions exceed their operational thresholds (Salam, 2020). These findings highlight the importance of resilience planning, particularly in regions with climatic extremes.

2.2. Climate Change and IoT Vulnerability: Global Trends and Specific Risks in Kazakhstan

The impact of climate change on IoT devices is attracting attention worldwide, but vulnerability is particularly pronounced in regions with significant seasonal and climatic extremes, such as Kazakhstan. IoT devices based on real-time data collection, monitoring and transmission are widely used in sectors such as agriculture, energy, urban infrastructure and transport. However, extreme weather events caused by climate change, such as heat waves, sudden cooling and seasonal variations, pose a significant risk to IoT devices, as highlighted in studies Atzori and Luigi (Atzori et al., 2010b). Studies conducted in arid regions show that exposure to extreme temperatures can lead to degradation of electronic components, changes in sensor accuracy, and even device failure (Soussi et al., 2024).

Kazakhstan, with its varied topography and strong climatic differences in different regions, presents a serious challenge for devices. Winter temperatures in northern regions can fall below -40°C , while summer temperatures in southern regions exceed 40°C . Such variations can subject devices to mechanical stresses that affect power consumption and functionality (Salnikov et al., 2023). Studies in Central Asia show that the increased frequency of extreme weather events in the region due to climate change may put more stress on IoT devices, increasing the risk of failure (World Bank, 2021). In addition, climate data projections for Kazakhstan indicate a trend towards warmer summers and colder winters with changing seasonal patterns, which could increase the strain on IoT systems if appropriate resilience measures are not taken.

The vulnerability of IoT devices to climate change in Kazakhstan is exacerbated by the region's unique environmental challenges, including extreme temperatures and an increase in the frequency and intensity of extreme weather events such as storms, heavy snowfall and droughts. Such environmental stresses disrupt the normal operation of IoT devices, especially those that rely on external sensors and power sources (Atzori et al., 2010b). For example, high temperatures can overheat and damage sensitive electronic components, while low temperatures can cause batteries to fail or sensors and communication systems to malfunction. In addition, seasonal variations, such as prolonged periods of extreme heat or cold, are an increasing challenge for IoT systems that must operate consistently throughout the year. In addition, the infrastructure that supports these devices, such as power grids and communication networks, can also be susceptible to weather fluctuations, further increasing the likelihood of device failures. Given the growing dependence of IoT systems on mission-critical operations in industries such as agriculture, transport and energy, robust adaptation strategies are needed to increase the resilience of these devices and ensure their reliability even in the most extreme weather conditions (Rastegari et al., 2023).

2.3. Climate-Related Specialties of Kazakhstan

Kazakhstan's climate is characterized by exceptional variability: winter temperatures can fall below -44°C in the north, while summer temperatures often exceed $+45^{\circ}\text{C}$ in southern deserts. Seasonal transitions are abrupt, with rapid shifts between hot summers and cold winters. In addition, the country faces frequent droughts, dust storms in arid regions, strong winds across the steppes, and heavy snow accumulation in the north and east (Kazhydromet, 2023). These environmental conditions create unique challenges for IoT systems, increasing the risk of failure due to freezing, overheating, moisture intrusion, or physical damage from storms.

2.4. Strategies for IoT Resilience to Harsh and Variable Environmental Conditions

Research on resilience strategies for IoT systems in harsh environments has focused on both technical and operational adaptation. Effective resilience strategies often include designing devices with components that can withstand a wider range of temperatures, collecting real-time data to dynamically adapt operations, and developing predictive maintenance protocols to ensure continuous functionality in variable environments. Raza and Saleem, for example, point out in their research the need for heat-resistant materials and adaptive power management to maintain device functionality at extreme temperatures (Raza et al., 2019). Other studies recommend implementing algorithms that adjust device settings based on environmental data to reduce power consumption and extend device life (Himeur et al., 2021).

In Kazakhstan, resilience strategies should consider not only temperature extremes but also other unique climatic factors such as early frosts, dry winds, and the rapid transition from summer to winter temperatures. For example, provisions to support the agricultural sector must consider the challenges of temperature fluctuations, droughts, and soil moisture fluctuations that affect crop health and resource allocation (Xenarios et al., 2018). IoT devices are also used in urban areas to monitor traffic and air quality, which requires robust sensor networks that can operate efficiently despite temperature fluctuations and seasonal changes in air quality (Gil et al., 2016). Studies in Central Asia show that without proactive measures to improve the resilience of IoT infrastructure, IoT may not provide accurate data, jeopardising public safety and economic stability (Riaz et al., 2023). Therefore, implementing adaptive algorithms, investing in heat-resistant devices, and utilising data-driven maintenance strategies are necessary to maintain IoT functionality in Kazakhstan's variable climate. In addition to technical solutions such as heat-resistant materials and adaptive algorithms, operational strategies in Kazakhstan should focus on integrating local weather data to predict environmental changes and adjust device settings in advance. For example, real-time monitoring of moistness and weather conditions can lead to automatic adjustment of irrigation systems, while predictive analytics can help predict extreme weather events so that IoT devices can go into energy-saving mode or shut down when weather conditions are not suitable (Pwavodi et al., 2024). Additionally, ensuring reliable connectivity between devices through redundant networks and backup systems is necessary to prevent data loss in the circumstance of extreme weather conditions (Gonçalves et al., 2024). By combining these adaptive approaches with a robust infrastructure, organisations can improve the overall resilience of IoT systems so that they can operate efficiently and provide accurate, real-time data despite the challenges posed by dynamic and extreme weather conditions.

2.5. Risk Modelling and Predictive Reliability Analysis of IoT Devices in Extreme Climatic Conditions

Quantifying climate-related risks for IoT devices is critical for predicting and mitigating potential failures. Climate risk models typically use environmental data to create risk curves that represent the probability of device failure under certain climatic conditions. However, while risk modelling is typically applied to physical infrastructure, research on risk assessment for IoT devices is relatively recent. Cote, Jean-Nicolas describe the use of risk assessment curves to identify critical temperature thresholds at which device performance may degrade. These models can be used to make operational decisions and design changes to improve device resilience (Cote et al., 2024).

For Kazakhstan, this approach is particularly relevant given the extreme and varying climatic conditions in different regions. The use of historical climate data, such as monthly averages of ERA5, allows risk modelling based on temperature and precipitation trends over decades (Copernicus Climate and Service, 2021). Studies focusing on Central Asia emphasise that risk curves can help identify device-specific thresholds at which performance problems are likely to occur, allowing for necessary changes in IoT deployment strategies (Parsons et al., 2023). By integrating real-time monitoring data and predictive analytics, these models allow for timely adjustments to IoT devices before environmental factors reach critical levels, thereby enhancing business continuity.

The potential for climate-related IoT disruptions also has implications for Kazakhstan's economy and public safety. For example, in agriculture, IoT devices play a key role in monitoring soil health, water consumption and pest control. Predictive risk models can help farmers optimise the use of devices, reducing the likelihood of failures during critical growing seasons. In urban infrastructure, air quality sensors, traffic management systems and energy monitoring devices depend on uninterrupted operation to maintain services and ensure safety. By predicting and mitigating risks by adapting to weather conditions, risk prediction models help create a more resilient IoT infrastructure that can cope with climate challenges in Kazakhstan. Additionally, incorporating predictive reliability analysis into IoT risk models allows organisations to take proactive actions, allowing them to anticipate and mitigate failures before they occur. For example, machine learning algorithms can be used to continuously update risk curves based on real-time data, improving the accuracy of predictions and providing valuable insights into long-term trends (Penalva, 2023). By taking into account local environmental variables such as wind speed, humidity, and snow level, these models can also provide a more complete picture of the complex factors affecting the performance of IoT devices. This approach not only improves the performance of IoT systems in Kazakhstan's harsh climate, but also facilitates cost-effective decision-making by optimising maintenance schedules, device replacement and resource allocation in industries such as agriculture, transport and energy. By continuously improving these models, Kazakhstan will be able to build a more robust and adaptable IoT infrastructure that can withstand the challenges of an extreme climate.

3. Methodology

This study employs a mixed-methods approach, integrating climate projection data with qualitative insights from interviews to develop a climate risk model for IoT device resilience in Kazakhstan. The methodology is organized into four key steps: data collection, device selection, climate risk modelling and data processing and visualization. These steps are designed to quantify the impact of extreme weather on IoT devices and propose adaptation strategies based on identified vulnerabilities.

3.1. Climate Data Collection

We used two main datasets:

ERA5 Reanalysis (Copernicus Climate Data Store):

Resolution: $0.25^\circ \times 0.25^\circ$ (approx. 30 km), hourly to monthly.

Period: 1940–2023.

Variables: near-surface temperature, relative humidity, precipitation, solar radiation, snow depth, and wind speed at 10 m.

Format: NetCDF (float32 datatype, gridded time series).

Processing: Bias correction was applied by comparing with national meteorological station data.

CMIP6 Climate Projections:

Scenarios: RCP4.5 (stabilization) and RCP8.5 (high emissions), with SSP5-8.5 used for extreme scenario analysis.

Period: 1950–2100.

Resolution: $0.5^\circ \times 0.5^\circ$, monthly means, downscaled for Kazakhstan.

Variables: same as ERA5 for consistency.

Data Type: NetCDF multidimensional arrays.

These datasets provided the quantitative basis for estimating the resilience of IoT devices to projected climate extremes.

We used climate projection data from the Coupled Model Intercomparison Project Phase 6 (CMIP6) to estimate the resilience of IoT devices to future climate extremes in Kazakhstan. CMIP6, the core dataset underpinning the 6th Assessment Report of the Intergovernmental Panel on Climate Change (IPCC), is an extended collection of global climate simulations. These simulations are the result of collaboration between leading climate research institutes using state-of-the-art general

circulation models (GCMs). CMIP6 data allow us to explore important scientific questions such as the predictability of the climate system, quantification of future climate change impacts, and uncertainties associated with different socioeconomic and emissions scenarios.

In particular, we used data from the SSP5-8.5 scenario, a high-emissions scenario characterised by rapid economic growth, high dependence on fossil fuels and minimal climate change mitigation. This 'business-as-usual' scenario is particularly useful for studying the extreme impacts of climate change because it predicts large increases in global temperature, more frequent and intense heat waves, more intense cold waves, and greater seasonal variability. These factors overlap with critical stressors for IoT devices in Kazakhstan, a region already exposed to extreme climate variability. All figures were created using Python, specifically using libraries like Matplotlib and NumPy. First, loaded the climate data from a NetCDF file with netCDF4, then extracted key variables like temperature, latitude, and longitude. Then selected a specific time period from the data and used a contour plot to visualize the temperature distribution.

The CMIP6 dataset used in this study includes two-dimensional and three-dimensional climate variables with high spatial and temporal resolution. These variables can be adapted to specific regions and periods to focus on different climate zones in Kazakhstan, from dry steppes to cold mountainous regions. SSP5-8.5 data were integrated into our climate risk models to estimate the probability of IoT device failure under different environmental conditions. For example, extreme temperatures exceeding operating thresholds can cause sensors, cameras and other IoT devices to malfunction or even fail completely. Similarly, high humidity or extreme temperature fluctuations can lead to condensation and degradation of materials, further limiting the functionality of devices.

To evaluate the potential impact of climate change on IoT devices in Kazakhstan, climate projections from CMIP6 models based on the RCP4.5 and RCP8.5 scenarios were used (IPCC, 2021). The Table 1 below summarises the key climate data, including changes in temperature and precipitation, used in the modelling to predict future conditions.

Table 1. Climate Data Ranges Specific to Kazakhstan and Central Asia.

<u>Climate Variable</u>	<u>Range (1950-2100)</u>	<u>Source</u>
Temperature (Kazakhstan)	1.5°C to 4.0°C increase	CMIP6 RCP4.5 & RCP8.5 (IPCC, 2021)
Winter Temperature	Increased frequency of extreme cold events (below -40°C)	CMIP6 RCP4.5 & RCP8.5 (IPCC, 2021)
Summer Temperature	Increased frequency of heatwaves (above 40°C)	CMIP6 RCP8.5 (IPCC, 2021)
Precipitation	-10% to +20% change	CMIP6 SSP5 Scenario
Extreme Heat Events	Increased frequency of heatwaves	CMIP6 RCP8.5 (IPCC, 2021)
Extreme Cold Events	Increased frequency of cold extremes	CMIP6 RCP4.5 & RCP8.5 (IPCC, 2021)

Risk curves help identify critical thresholds, for example points where the probability of failure increases dramatically if climate conditions differ from the normal range. For IoT sensors used for agricultural monitoring, for example, a temperature deviation of ± 10 °C from the design range can significantly increase the probability of failure and require additional protective measures such as isolation mechanisms or cooling.

3.2. IoT Device Selection and Priorities

The selection of IoT devices was based on their relevance to Kazakhstan's critical sectors: agriculture, energy, transport, and urban infrastructure. We prioritized devices widely deployed outdoors, where exposure to climate stress is highest.

Selection priorities included: relevance to national infrastructure (agricultural sensors, energy monitoring devices, POS terminals); exposure to harsh outdoor conditions (routers, cameras, actuators); sectoral representativity (covering at least one device type from each critical sector); comparability with international studies to allow benchmarking of resilience strategies.

Regarding connectivity devices, we initially included SIM cards because they remain widely used in Kazakhstan. However, we acknowledge the transition toward e-SIM technology, which may provide improved durability and flexibility. This aspect is now discussed in the revised manuscript to reflect technological trends and alternatives.

3.3. IoT Device Operating Conditions

Based on the climate risk projections described above, it is important to determine the operating conditions and performance thresholds of the IoT devices used in this study. The Table 2 below summarises the typical operating ranges of these devices, including cameras, sensors, actuators and others, to determine risk assessment thresholds and identify environmental factors that may affect device functionality in future climate conditions. The operating temperature ranges are based on manufacturer specifications for each IoT device type. Differences between ranges reflect design considerations: devices intended for outdoor use (e.g., sensors, cameras) are manufactured with wider tolerances to withstand environmental stress, while devices primarily used in sheltered settings (e.g., POS terminals) have narrower ranges.

Table 2. Operating Conditions and Ranges of Used IoT Devices.

IoT Device Type	Operating Temperature Range	Operating Humidity Range	Power Requirements	Snow/Ice Resistance	Wind Resistance	Common Applications
Cameras (Outdoor)	-30°C to 50°C	10% to 100%	Medium (5V, 12V DC)	Moderate (icing risk)	Up to 20 m/s	Security, environmental monitoring
Sensors (Temperature, Humidity)	-40°C to 55°C	0% to 100%	Low (battery powered or low voltage)	Low-moderate (indoor/outdoor)	Low	Smart homes, agriculture, weather monitoring
Actuators (Valve Controllers)	-30°C to 60°C	0% to 100%	Medium (12V DC)	Moderate	Moderate	Industrial systems, irrigation
Routers (IoT Gateways)	-30°C to 50°C	5% to 95%	High (AC/DC, 12V)	Low	Moderate	Smart homes, IoT infrastructure
POS Terminals (Outdoor)	-30°C to +50°C	10% to 100%	Medium (AC/DC, 12V)	Moderate (weatherproof, dustproof)	Low	Retail, payment systems, outdoor kiosks, mobile sales
SIM Cards (for IoT)	-40°C to +55°C	0% to 100%	Low (powered by device)	N/A	N/A	Mobile devices, data communication, IoT connectivity
e-SIM	-40°C to +85°C	0% to 100%	Low	N/A	N/A	Next-gen IoT connectivity

By combining high-resolution CMIP6 climate projections, we extended these risk models to estimate the future probability of failure based on predicted conditions, such as the increase in intensity of heat waves by mid-century. The integration of CMIP6 data also allowed us to create a spatial map of these risks across Kazakhstan, highlighting the region's most prone to IoT device failures. Such maps are essential for policymakers and stakeholders to prioritise resilience building in critical sectors such as agriculture, energy and transport.

Overall, the use of CMIP6 data, particularly the SSP5-8.5 scenario, provided a solid basis for understanding the potential impacts of extreme climate scenarios on IoT devices in Kazakhstan. The combination of climate projections, modelling of device failure probability and regional mapping provides practical insights to help industry adapt IoT systems to the challenges of climate change.

Another data collection method was used in this research is the qualitative data from interviews. To contextualize the quantitative data, we conducted interviews with related organizations, including IoT developers, climate scientists, and professionals in sectors reliant on IoT devices, such as transportation, logistics, agriculture. These interviews provide insights into the specific operational challenges faced by IoT devices in Kazakhstan's climate, as well as current adaptation strategies and potential areas for improvement. Interview responses were conducted thematically, with a focus on identifying common concerns related to temperature fluctuations, device maintenance, and reliability in extreme weather conditions.

The second step involves data analysis. We will first discuss statistical methods for analysing climate trends, followed by a thematic analysis of interview data.

The historical and projected climate data from ERA5 are subjected to statistical analysis to identify trends in temperature extremes, seasonal shifts, and precipitation patterns. This analysis includes calculating mean, minimum, and maximum values, as well as examining variability across different regions (Yilmaz, 2023). Given Kazakhstan's distinct climate zones, regional analysis is essential for capturing localized impacts. Statistical tests, such as t-tests or Mann-Kendall trend tests, are used to verify the significance of observed changes in climate variables over time.

The thematic analysis method was used to analyse the interview data.

Interview data is analysed using thematic coding to extract recurrent themes regarding IoT resilience issues. Key themes include temperature thresholds for device failure, challenges related to power supply in remote areas, and maintenance difficulties during extreme weather events. This qualitative analysis supports the quantitative findings by offering a grounded perspective on how climate conditions impact IoT functionality in the organisations among Kazakhstan.

3.4. Climate Risk Modelling

The next important step is to conduct climate risk modelling. How was the development of risk estimate curves carried out? The core of this study's analysis involves developing risk estimate curves, which quantify the probability of IoT device failure under varying climate conditions. Using historical climate data, we define threshold values for environmental variables, such as temperature and humidity, beyond which device performance is likely to degrade. These thresholds are determined based on both literature (Yilmaz, 2023) and (Copernicus Climate and Service, 2021) the operational parameters of IoT devices obtained from industry reports.

We developed risk curves based on device operating ranges and climate variables. Probability of failure was calculated as:

$$P(\text{failure}) = \int_{x \notin R} f(x) dx$$

where $f(x)$ is the kernel density estimation (KDE)-based probability density function of temperature or humidity, and R is the device's operating range. Sensitivity tests were conducted with threshold shifts of ± 5 °C and ± 10 % humidity.

The risk estimate curves are constructed by mapping device performance data against temperature and humidity thresholds. For example, sensors may operate optimally within a specified temperature range, but performance may decline or fail entirely as temperatures exceed these limits. By using failure probability distributions, we create curves that illustrate the likelihood of device failure as climate variables deviate from baseline operational ranges.

How did we conduct the validation and sensitivity testing? To ensure the accuracy of the risk estimate curves, we conduct sensitivity testing by adjusting input variables and assessing the resulting changes in failure probability. This step allows us to understand the robustness of our model and identify the environmental conditions that most significantly affect device reliability. Validation of the model is performed using cross-validation techniques, where data subsets are analysed separately to compare the consistency of risk estimates.

Next is the time for the Integration with Climate Projections, let us discuss this. Finally, to forecast the future impact of climate change on IoT devices, we integrate ERA5 climate projections into the model. By applying projected climate scenarios to the risk estimate curves, we assess how the likelihood of device failure may change under predicted climate conditions. This integration enables a forward-looking analysis, providing estimates of IoT reliability under potential future scenarios, such as increased frequency of heatwaves or colder winter extremes.

3.5. Data Processing and Visualization

The final important step is mapping and visualization. To effectively display the spatial distribution of climate risks, data analysis and visualization, Python was used. Beyond Matplotlib and NumPy, the following libraries were employed:

Pandas (data handling, time series analysis).

netCDF4 (extraction of ERA5 and CMIP6 NetCDF files).

Seaborn (statistical plotting, KDE).

SciPy (statistical tests: t-test, Mann–Kendall trend analysis).

Cartopy (geospatial mapping with correct projections and scale bars).

All figures were revised to include error bars, improved legends, probability density function (PDF) definitions, and professional cartographic standards for maps. By leveraging Python's data visualization libraries, we overlaid risk data onto regional maps, illustrating which areas are most likely to experience operational challenges with IoT devices. These visualizations emphasize regions vulnerable to climate impacts, helping policymakers and industry stakeholders prioritize areas for resilience planning and adaptation investments.

Section 4.

Analysis and Results

As this research paper employed both quantitative and qualitative data collection methods to analyse the climate risks affecting IoT devices in Kazakhstan, the integration of statistical climate data and insights from interviews provided a understanding of the operational challenges, adaptation strategies, and potential risks IoT devices face in the context of Kazakhstan's varied climate conditions.

To complement the quantitative climate projections, we collected qualitative data through semi-structured interviews designed to capture sector-specific insights into IoT resilience under extreme weather conditions.

Timing: Interviews were conducted between May 2023 and February 2024.

Participants: A total of 20 respondents participated, representing a balance of IoT developers, sector specialists, and managers in the fields of agriculture, transport, energy, and logistics.

Rationale for sector selection: These sectors were prioritized because they rely heavily on outdoor IoT devices that are directly exposed to Kazakhstan's harsh climate, making them highly vulnerable to weather-related disruptions.

Representativity: Participants were chosen to provide diverse perspectives, ensuring coverage of both technical experts (who understand device performance and limitations) and operational managers (who face real-world deployment and maintenance challenges).

Extreme weather experience: The majority of respondents had direct experience with device failures or operational disruptions during heatwaves, severe frosts, snow accumulation, or dust storms.

IoT adoption stage: Respondents included both current users of IoT devices (e.g., agricultural sensors, smart irrigation systems, power grid monitors) and organizations planning future IoT integration, enabling the study to capture both present challenges and anticipated risks.

Analysis approach: Interview transcripts were thematically coded, focusing on:

Climate-related device failures (battery issues, sensor inaccuracies, casing damage).

Maintenance and calibration challenges in remote or extreme environments.

Sector-specific resilience strategies, including redundancy, weatherproofing, and predictive maintenance.

This qualitative dataset complements the climate modelling by grounding statistical risk curves in the lived experiences of practitioners and ensuring that the resilience framework reflects both scientific projections and operational realities.

The analysis of historical and projected climate data from ERA5 revealed significant trends in temperature extremes, seasonal shifts, and precipitation patterns across different regions of Kazakhstan. To visualize the temperature distributions across different regions of Kazakhstan we have created a graph for temperature distribution and risk zones this is also to assess the potential risk zones for IoT device operation under both historical and future climate scenarios. By plotting the probability density of temperatures and highlighting areas that fall outside the operational limits of IoT devices (e.g., -30°C to $+30^{\circ}\text{C}$), the graph provides a clear representation of where and when devices are most vulnerable to extreme weather conditions. This method allows for a detailed analysis of the climatic stresses on IoT devices, helping to identify high-risk areas and facilitating the development of targeted resilience techniques to avoid device failure in extreme climates (Figure 1). This graph illustrates regions of Kazakhstan where temperatures are likely to exceed the operational limits of IoT devices, increasing the risk of failure. The probability density highlights the frequency of extreme temperatures and regional climatic variations. This information helps identify high-risk areas and prioritize resilience strategies, such as protective measures and alternative deployment options to ensure device functionality in extreme weather. This localized analysis provided insights into how different IoT devices might perform in response to specific regional climate conditions.

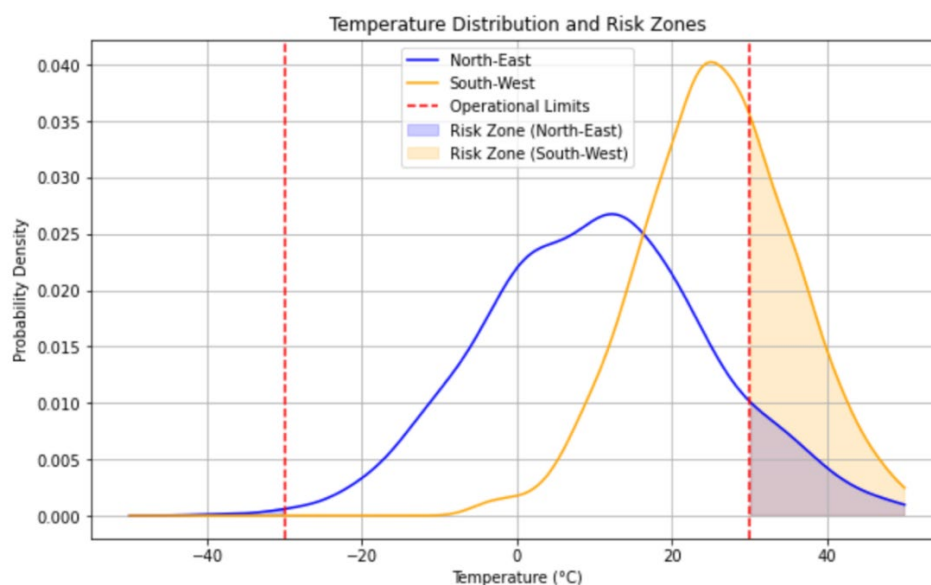


Figure 1. Temperature distribution and risk zones.

Next, we compare temperature probability density functions for four regions of Kazakhstan - north, south, east and west - using the Kernel Density Estimation (KDE) method to smooth temperature distributions. By plotting these curves, the graph visualises regional climate changes and highlights temperatures that are outside the operating limits of IoT devices (-30°C to $+30^{\circ}\text{C}$). This allows us to visualize comparison of how a region's climate can affect the functionality of IoT devices and identifies high-risk areas that require targeted resilience strategies to mitigate the impact of extreme temperatures (Figure 2).

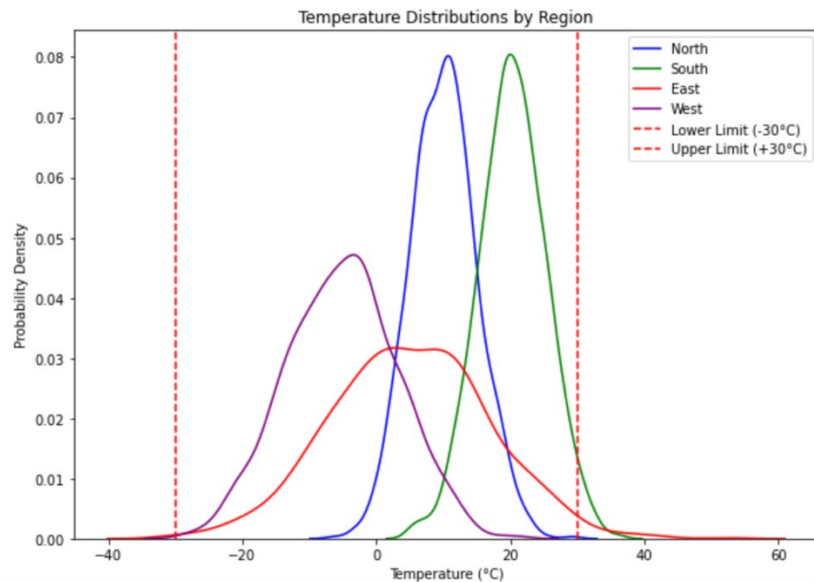


Figure 2. Temperature distribution by region.

Figure 3 represents temperature distributions for historical and projected climate scenarios in different regions of Kazakhstan, Kernel Density Estimation (KDE) method has been applied to smooth the data. Identifying temperatures outside the operating range of IoT devices (-30°C to $+30^{\circ}\text{C}$) highlights areas where the risk of device failure due to extreme weather is highest. This analysis highlights regional climate change and offers strategies to enhance the resilience of IoT devices in vulnerable areas, ensuring their reliable operation in future climate conditions.

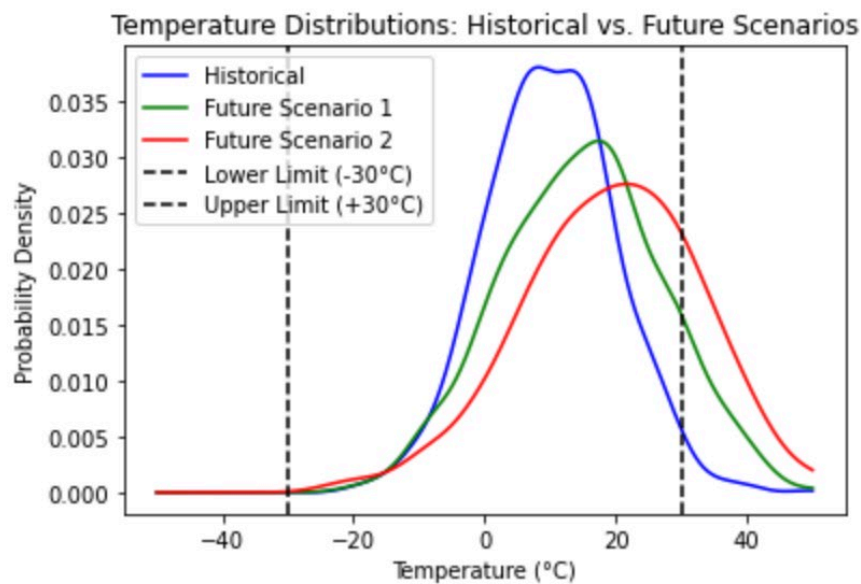


Figure 3. Temperature distributions: historical and future scenarios.

To identify and visualize the regions in Kazakhstan where IoT devices are most at risk of failure due to extreme temperatures risk analysis has been implemented. The probability density approach provided an effective way to capture the likelihood of temperature extremes beyond device operating thresholds. To complement density plots, we added an alternative visualization in the form of a heatmap, which illustrates the spatial distribution of IoT device failure probabilities across Kazakhstan. This heatmap allows clustering of regions with similar risk levels, highlighting hotspots where resilience strategies should be prioritized (Figure 4). To create the graph, we calculated the percentage at risk for IoT devices in different regions by analysing the temperature distributions using kernel density estimation (KDE). This involves integrating the probability density to determine the area outside the operating temperature range (-30°C to $+30^{\circ}\text{C}$) and dividing by the total area to determine the percentage at risk. A graph is created for historical and future climate scenarios, providing a comparative overview of how the risks of IoT device failure change with climate change. This visualisation highlights high-risk regions and helps prioritise strategies to improve device resilience to extreme climate conditions.

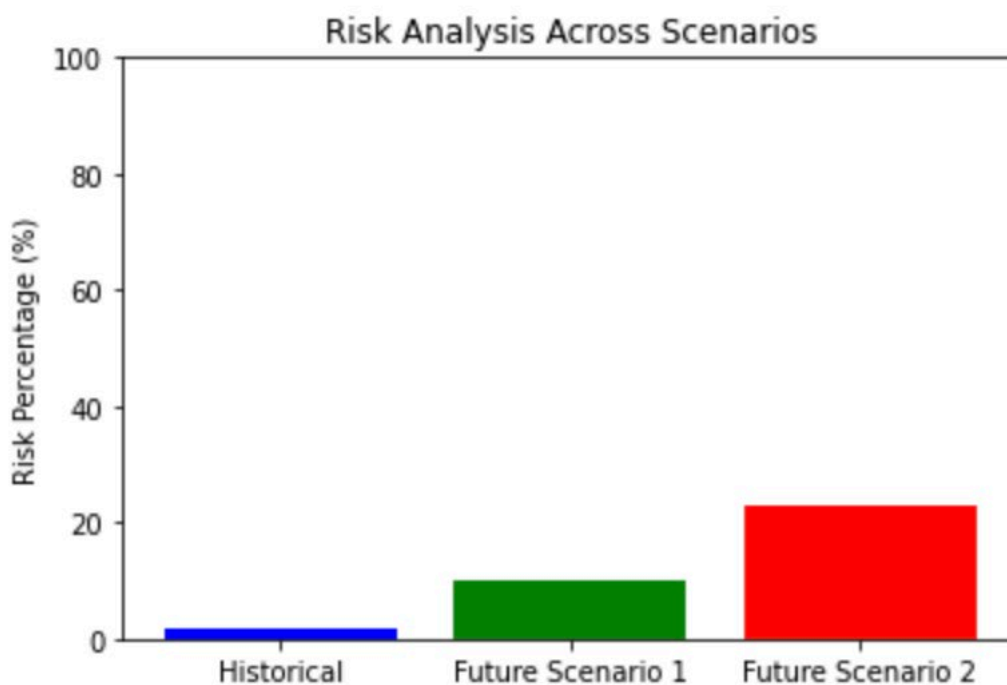


Figure 4. Risk analysis across different scenarios.

To assess the vulnerability of IoT devices to extreme weather conditions, we have developed risk curves that visualise the probability of device failure based on temperature distribution. Figure 5 displays four regions to provide more detailed analysis of temperature distribution and IoT device risk allowing for a deeper examination of each region's different specific condition. The process begins with the collection of temperature data for specific regions (e.g. North, South, East and West Kazakhstan) from reliable sources such as ERA5 or CMIP6 climate projections. These data include historical and future scenarios, allowing us to analyse both current and projected risks.

Using the kernel density estimation (KDE) method, we smoothed the temperature distributions to create continuous probability density functions (PDFs). These PDFs illustrate the probability of occurrence of different temperature ranges in each region. The operating limits of IoT devices, which are usually defined as -30°C to $+30^{\circ}\text{C}$, are used as thresholds to define risk zones, i.e. areas where temperatures exceed these limits.

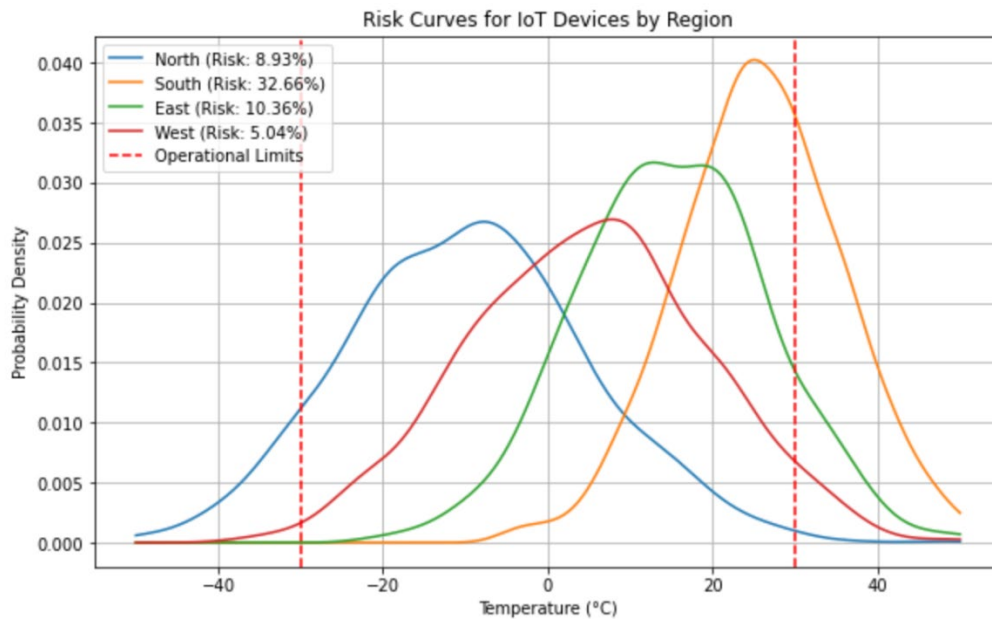


Figure 5. Risk curves by region for IoT devices.

The next step is to calculate the percentage of PDF that falls outside of these operating limits. This is done by integrating the density function in the risk zones and normalising with respect to the total area under the curve. The result is expressed as a risk percentage indicating the probability of equipment failure due to temperature extremes in each region.

Finally, risk curves are plotted for each region, showing the probability density of temperatures along with the operating limits markers. This visualisation highlights the frequency and severity of extreme temperature events and allows for a clear comparative analysis between regions. These risk curves are essential for identifying high-risk areas and developing strategies to improve the resilience of IoT devices to changing climate conditions.

The qualitative data from interviews with IoT specialists, climate scientists, and professionals in sectors reliant on IoT devices, such as transportation, logistics, and agriculture, provided valuable insights into the operational challenges faced by IoT devices (Figure 6).

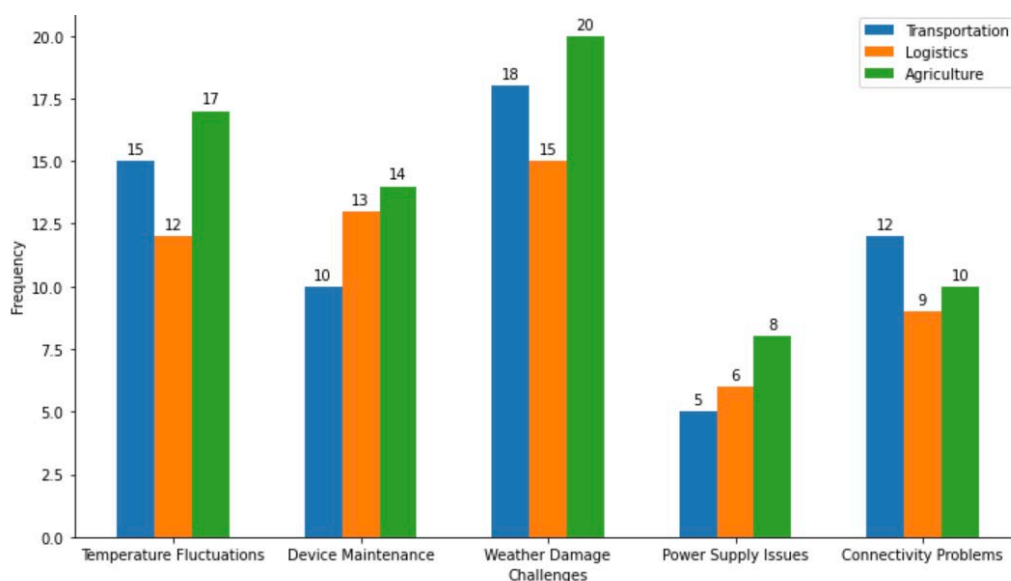


Figure 6. Challenges faced by IoT devices in different sectors according to interview results (20 respondents).

As the core of this research involved developing risk estimate curves to quantify the probability of IoT device failure under different climate conditions we analysed historical climate data, and defined threshold values for temperature and humidity beyond which device performance is likely to degrade. These thresholds were derived from both literature (Yilmaz, 2023) and manufacturer specifications for IoT devices (Copernicus Climate and Service, 2021) as mentioned in previous section. Risk estimate curves were constructed by mapping device performance data against environmental variables, such as temperature and humidity. For instance, sensors typically perform optimally within a specified temperature range, but their performance declines or fails when exposed to extreme temperatures. The resulting curves demonstrate the likelihood of failure as climate variables deviate from these baseline operational ranges (Figure 7).

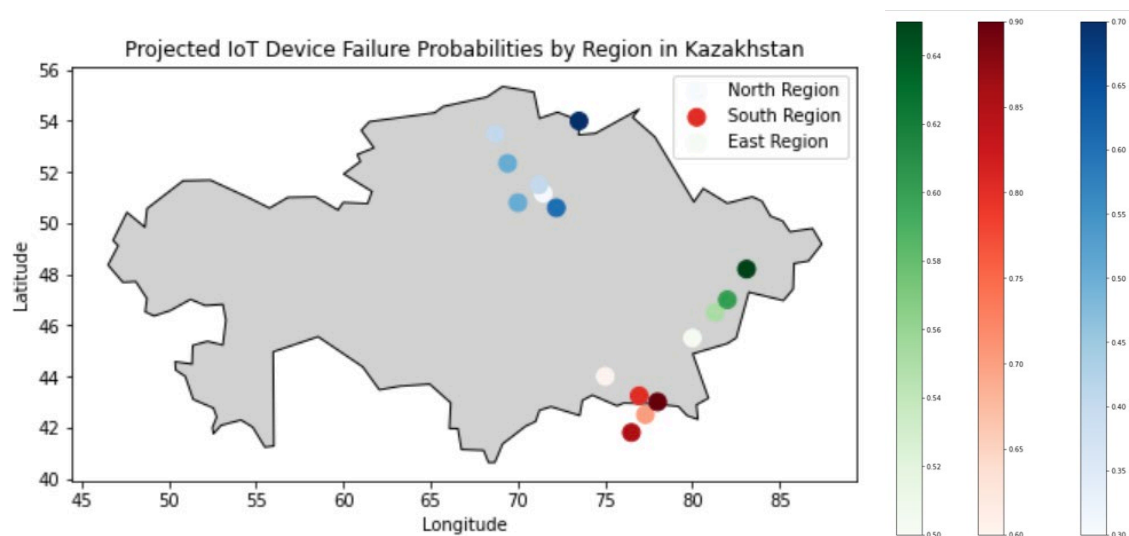


Figure 7. Climate projection risks for IoT devices by region until 2040.

The findings from this research provide an assessment of the climate risks IoT devices face in Kazakhstan (Figure 6, 7). Through a combination of quantitative climate data analysis, qualitative interview insights, and risk modelling, we have identified key challenges and vulnerabilities in IoT systems under current and future climate conditions. These insights will help guide policymakers, organisations, and IoT developers in creating targeted adaptation strategies to enhance the resilience of IoT devices in Kazakhstan's climate. The use of risk estimate curves, integrated with climate projections, offers a valuable tool for forecasting future challenges and planning for climate-resilient IoT infrastructure. The visualizations produced in this study will be instrumental in identifying priority areas for investment in climate adaptation measures.

5. Conclusion

In conclusion, this study assessed the vulnerability of Internet of Things (IoT) devices in Kazakhstan to climate extremes by integrating ERA5 and CMIP6 climate projections with device operating thresholds and stakeholder interviews. The results demonstrate that IoT systems face increasing risks from temperature extremes, humidity fluctuations, and additional stressors such as solar radiation, windstorms, heavy snowfall, and droughts. Our findings show that northern Kazakhstan is most vulnerable to severe cold events, while southern and central regions face heightened risks from prolonged heatwaves. These climatic pressures significantly increase the probability of device malfunctions, particularly in sensors, cameras, routers, and POS systems. Interviews confirmed that stakeholders are concerned about maintenance difficulties, calibration errors under extreme conditions, and unreliable power supply in remote areas. Several resilience strategies emerged from this research. Technical measures include designing hardware with extended operating ranges, protective casings, and adaptive energy management. Operational

measures involve predictive maintenance, redundancy in communication networks, and climate-informed deployment planning. Together, these approaches can enhance device performance and reduce operational downtime under extreme conditions. The integration of risk modelling, probability density functions, and spatial risk mapping provides policymakers and industry stakeholders with a practical framework to anticipate IoT failures and prioritize adaptation investments. By identifying regional “hotspots” of vulnerability, decision-makers can allocate resources more effectively to safeguard critical sectors such as agriculture, energy, and urban infrastructure. This study has three important implications: Policy and planning: National IoT strategies should include climate resilience standards, informed by risk projections. Research and development: Device design must incorporate tolerance to multiple stressors, including radiation, wind, and snow, not just temperature and humidity. Future studies: Expanding validation with real-world device failure data and comparing resilience strategies across Central Asia will enhance model accuracy and regional relevance. In conclusion, IoT devices in Kazakhstan are highly vulnerable to projected climate extremes, but with targeted technical and operational adaptations, resilience can be significantly improved. The methodology developed here offers a transferable framework for other Central Asian countries facing similar challenges, contributing to the broader agenda of building climate-resilient digital infrastructures.

Funding: "Bolashaq" Scholarship of the Republic of Kazakhstan.

References

1. ALGARNI, S. & NUTTER, D. 2015. Influence of Dust Accumulation on Building Roof Thermal Performance and Radiant Heat Gain in Hot-Dry Climates. *Energy and Buildings*, 104, 181-190.
2. ATZORI, L., IERA, A. & MORABITO, G. 2010a. The Internet of Things: A survey. *Computer Networks*, 54, 2787-2805.
3. ATZORI, L., IERA, A. & MORABITO, G. 2010b. The Internet of Things: A Survey. *Computer Networks*, 2787-2805.
4. COPERNICUS CLIMATE & SERVICE, C. 2021. ERA5: Fifth generation of ECMWF atmospheric reanalyses of the global climate.
5. COTE, J.-N., GERMAIN, M., LEVAC, E. & LAVIGNE, E. 2024. Vulnerability assessment of heat waves within a risk framework using artificial intelligence. *Science of The Total Environment*, 912, 169355.
6. GIL, D., FERRÁNDEZ, A., MORA-MORA, H. & PERAL, J. 2016. Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services. *Sensors*, 16, 1069.
7. GONÇALVES, A. C. R., COSTOYA, X., NIETO, R. & LIBERATO, M. L. R. 2024. Extreme weather events on energy systems: a comprehensive review on impacts, mitigation, and adaptation measures. *Sustainable Energy Research*, 11, 4.
8. HIMEUR, Y., GHANEM, K., ALSALEMI, A., BENSALI, F. & AMIRA, A. 2021. Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives. *Applied Energy*, 287, 116601.
9. IPCC 2021. IPCC Sixth Assessment Report.
10. KAZHYDROMET 2023. national hydrometeorological service of the Republic of Kazakhstan.
11. KAZHYDROMET.KZ 2023. The national hydrometeorological service of the Republic of Kazakhstan.
12. OTHMANE FRIHA, M. A. F., LEI SHU, LEANDROS MAGLARAS, XIAOCHAN WANG 2021. Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies. *IEEE/CAA Journal of Automatica Sinica*, 8, 718.
13. PANDIYAN, P., SARAVANAN, S., KANNADASAN, R., KRISHNAVENI, S., ALSHARIF, M. H. & KIM, M.-K. 2024. A comprehensive review of advancements in green IoT for smart grids: Paving the path to sustainability. *Energy Reports*, 11, 5504-5531.
14. PARSONS, E., PANAOUSIS, E., LOUKAS, G. & SAKELLARI, G. 2023. A Survey on Cyber Risk Management for the Internet of Things. *Applied Sciences*, 13, 9032.

15. PENALVA, M., RUIZ, C., MARTÍNEZ, V., VEIGA, F., VEIGA, F., & BALLESTEROS, T. 2023. Application-Oriented Data Analytics in Large-Scale Metal Sheet Bending. *Applied Sciences*, , 13187.
16. PWAVODI, J., IBRAHIM, A. U., PWAVODI, P. C., AL-TURJMAN, F. & MOHAND-SAID, A. 2024. The role of artificial intelligence and IoT in prediction of earthquakes: Review. *Artificial Intelligence in Geosciences*, 5, 100075.
17. RAHMANI, H., SHETTY, D., WAGIH, M., GHASEMPOUR, Y., PALAZZI, V., CARVALHO, N. B., CORREIA, R., COSTANZO, A., VITAL, D., ALIMENTI, F., KETTLE, J., MASOTTI, D., MEZZANOTTE, P., ROSELLI, L. & GROSINGER, J. 2023. Next-Generation IoT Devices: Sustainable Eco-Friendly Manufacturing, Energy Harvesting, and Wireless Connectivity. *IEEE Journal of Microwaves*, 3, 237-255.
18. RASTEGARI, H., NADI, F., LAM, S. S., IKHWANUDDIN, M., KASAN, N. A., RAHMAT, R. F. & MAHARI, W. A. W. 2023. Internet of Things in aquaculture: A review of the challenges and potential solutions based on current and future trends. *Smart Agricultural Technology*, 4, 100187.
19. RAZA, S., FAHEEM, M. & GÜNES, M. 2019. Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges-A MAC survey. *International Journal of Communication Systems*, 32, e4074.
20. RIAZ, K., MCAFEE, M. & GHARBIA, S. S. 2023. Management of Climate Resilience: Exploring the Potential of Digital Twin Technology, 3D City Modelling, and Early Warning Systems. *Sensors*, 23, 2659.
21. SALAM, A. 2020. Internet of Things for Environmental Sustainability and Climate Change.
22. SALNIKOV, V., TALANOV, Y., POLYAKOVA, S., ASSYLBEKOVA, A., KAUAZOV, A., BULTEKOV, N., MUSRALINOVA, G., KISSEBAYEV, D. & BELDEUBAYEV, Y. 2023. An Assessment of the Present Trends in Temperature and Precipitation Extremes in Kazakhstan. *Climate*, 11, 33.
23. SOUSSI, A., ZERO, E., SACILE, R., TRINCHERO, D. & FOSSA, M. 2024. Smart Sensors and Smart Data for Precision Agriculture: A Review. *Sensors*, 24, 2647.
24. WORLD BANK, G. A. T. A. D. B. 2021. Climate Risk Country Profile: Kazakhstan
25. XENARIOS, S., SMAKHTIN, V., SEHRING, J., SCHMIDT-VOGT, D., TSANI, S., HANNAH, C. & MICHALENA, E. 2018. Water-Energy-Food Nexus and Environment in Central Asia.
26. XU, L. D., HE, W. & LI, S. 2014. Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, 10, 2233-2243.
27. YILMAZ, M. 2023. Accuracy assessment of temperature trends from ERA5 and ERA5-Land. *Science of The Total Environment*, 856, 159182.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.