Security Risks

Scope

EVERSION Technologies has developed a system aimed at efficiently collecting, storing, and processing sensor data. This solution includes a mobile application that connects to sensors via Bluetooth, retrieves measured values, and transmits them to the backend for storage and further processing. Authentication services from Firebase are integrated into the mobile application to facilitate user registration and authentication before accessing its functionalities.

Furthermore, the company's public website serves as a valuable resource, providing general information about their products. The website also hosts a user-centric dashboard that displays all measurements. Firebase authentication services are implemented in the web application to ensure secure access for users. All user and measurement data are stored in the backend databases.

The scope of all possible security risks outlined in this document encompasses all the aforementioned components. Specifically, it includes the sensors themselves, the mobile application, the company website, the Firebase authentication service and the Firestore database, the backend server and the backend databases (InfluxDB for storing raw sensor data, MongoDB for storing aggregated data).

Confidentiality

Sensors

- Hackers may attempt to intercept communication between sensors and the mobile application, gaining access to sensitive data such as measurements or user information.

Mobile Application

- Insecure storage of sensitive data on the device could lead to data leakage if the device is lost, stolen, or compromised.
- Weak encryption or lack of encryption during data transmission could expose sensitive information to interception by unauthorized parties.
- Malicious apps or attackers with physical access to the device could capture sensitive information displayed by the mobile application.

Web application

- Lack of HTTPS or weak encryption during data transmission could expose sensitive information to interception by attackers.

- Improper error handling or misconfigurations may lead to the disclosure of sensitive information through error messages or debugging interfaces.
- Vulnerabilities such as SQL injection or improper input validation could allow attackers to retrieve sensitive data stored in the backend databases.
- Attackers could use phishing techniques to trick users into divulging their credentials or other sensitive information.

Firebase Authentication Service and database

- Misconfigurations or inadequate access controls in Firestore databases could result in unauthorized access to sensitive user data, leading to data leakage and confidentiality breaches.
- Lack of encryption for data at rest or in transit could expose sensitive information to unauthorized access or interception.

Backend Server and Databases

- Weak authentication mechanisms or misconfigured access controls could lead to unauthorized access to sensitive data stored in the backend databases, resulting in data breaches and confidentiality violations.
- Lack of encryption for data transmission between the backend server and databases could expose sensitive information to interception.
- Malicious insiders with access to the backend server or databases could steal or leak sensitive data.

Integrity

Sensors

- Malicious actors might try to tamper with sensor data either in transit or at rest, leading to inaccurate measurements or false readings being recorded.
- Attackers could attempt to modify the firmware of sensors, compromising the integrity of the data collected or causing the sensors to behave unpredictably.

Mobile Application

- If the mobile application does not implement proper integrity checks, attackers could modify data in transit or on the device, leading to integrity violations.
- Attackers could intercept and modify data exchanged between the mobile application and backend servers, compromising data integrity.
- Lack of proper permissions or security controls may allow unauthorized modifications to the application's code or configuration, leading to integrity issues.

Web application

- Vulnerabilities such as SQL injection or improper input validation could allow attackers to tamper with data stored in the backend databases, compromising integrity.

Firebase Authentication Service and database

- Vulnerabilities such as injection attacks, IDOR, or weak input validation could allow attackers to manipulate data stored in the database.
- Inadequate access controls or weak authentication mechanisms could lead to unauthorized modifications of data.
- Failure to implement proper auditing and monitoring could hinder the detection of unauthorized changes to data.

Backend Server and Databases

- Vulnerabilities such as injection attacks, IDOR, or weak input validation could allow attackers to manipulate data stored in the database.
- Inadequate access controls or weak authentication mechanisms could lead to unauthorized modifications of data.
- Failure to implement proper auditing and monitoring could hinder the detection of unauthorized changes to data.

Availability

Sensors

- Hackers may launch DoS attacks against sensors, flooding them with excessive requests or malicious traffic, causing them to become unresponsive and affecting data collection.
- Physical attacks on the sensors, such as vandalism or destruction, could render them inoperable, leading to a loss of availability.

Mobile Application

- Vulnerabilities or bugs in the mobile application's code could lead to crashes or errors, affecting its availability to users.

Web application

- Attackers may attempt to overwhelm the web application with excessive traffic, leading to a degradation or complete loss of availability for legitimate users.
- Vulnerabilities such as inefficient code, lack of rate limiting, or insufficient resource allocation could lead to resource exhaustion, affecting the availability of the web application.

Firebase Authentication Service and database

- Downtime or disruptions to the Firebase authentication service could impact the availability of user authentication functionality, affecting the overall availability of the system.
- Attackers may target Firebase services or Firestore databases with DoS attacks, leading to service disruptions and availability issues.

Backend Server and Databases

- Attackers may launch DoS attacks against the backend server or databases, flooding them with excessive traffic or requests and causing service disruptions or downtime.
- Hardware failures, software bugs, or misconfigurations could lead to backend failures or crashes.

Authenticity

Sensors

- Attackers may attempt to impersonate legitimate sensors by spoofing their identities, leading to unauthorized access to the system or the injection of falsified data.

Mobile Application

- Malicious actors could create fake versions of the mobile application to deceive users into providing sensitive information.

Web application

- Vulnerabilities in session management could allow attackers to fixate session IDs and impersonate legitimate users.
- Lack of CSRF protections could allow attackers to forge requests on behalf of authenticated users, leading to unauthorized actions and compromising authenticity.

Firebase Authentication Service and database

- Weak authentication mechanisms or credential stuffing attacks could result in unauthorized access to user accounts.
- Vulnerabilities in token handling or session management could allow attackers to manipulate authentication tokens or sessions.

Backend Server and Databases

- Weak authentication mechanisms or insufficient identity verification measures could allow attackers to impersonate legitimate users or the backend system.

Accountability

Sensors

- Inadequate logging mechanisms within the sensors may lead to a lack of accountability, making it difficult to trace and attribute security incidents or unauthorized access.

Mobile Application

- If the mobile application does not maintain accurate audit logs, attackers could manipulate or delete logs to cover their tracks, compromising accountability.

Web application

- Insufficient logging of user actions or system events may hinder the ability to track and attribute security incidents.
- Attackers could manipulate or delete audit logs to cover their tracks and evade detection.

Firebase Authentication Service and

- Inadequate logging or auditing mechanisms in Firebase authentication service or Firestore databases could hinder the ability to track and attribute security incidents.
- Failure to monitor user activity or system events could result in undetected security breaches or unauthorized access.

Backend Server and Databases

- Inadequate logging or auditing mechanisms in the backend server or backend databases could hinder the ability to track and attribute security incidents.
- Failure to monitor user activity or system events could result in undetected security breaches or unauthorized access.

Access Control

Sensors

- Inadequate access controls may result in unauthorized individuals gaining access to the sensors.
- Failure to change default credentials or weak password policies could expose sensors to brute-force attacks or unauthorized access.

Mobile Application

- Attackers may attempt to modify the mobile application's code to inject malicious functionality or bypass security controls.

- Insecure authentication mechanisms could allow attackers to gain unauthorized access to the mobile application, compromising access control.
- Inadequate access controls within the application could allow users to access unauthorized functionality or data of other users.
- Flaws in session management could lead to session hijacking or unauthorized access to other user accounts.

Web Application

- Weak password policies, lack of multi-factor authentication, or improper handling of authentication tokens could lead to unauthorized access to the web application.
- Failure to enforce proper (vertical) access controls could allow unauthorized users to access sensitive functionality or data within the web application.
- Insufficient validation of user permissions or improper session management could enable attackers to (horizontally) abuse their privileges within the web application.

Firebase Authentication Service and database

- Misconfigurations or weak access controls in Firebase authentication service or Firestore database could allow unauthorized users to access sensitive data or perform privileged actions.
- Vulnerabilities that enable attackers to (vertically) escalate their privileges within Firebase authentication service or Firestore database could lead to unauthorized access to sensitive functionality or data.
- Insecure cross-account access configurations could result in unauthorized (horizontal) access to Firebase or Firestore resources.

Backend Server and Databases

- Misconfigurations or weak access controls in the backend server or backend databases could allow unauthorized users to access sensitive data or perform privileged actions.
- Vulnerabilities that enable attackers to (vertically) escalate their privileges within the backend server or backend databases could lead to unauthorized access to sensitive functionality or data.
- Insecure cross-account access configurations could result in unauthorized (horizontal) access to backend resources.

Safety

Sensors

- Failure of the sensor could potentially endanger users or the surrounding environment physically.