|  |  |  |
| --- | --- | --- |
|  | دانشکده مهندسی کامپیوتر و فناوری اطلاعات | F:\Arm\AKUT.svg.png |

آزمایشگاه اینترنت اشیاء

گروه پلتفرم

**عنوان سند:**

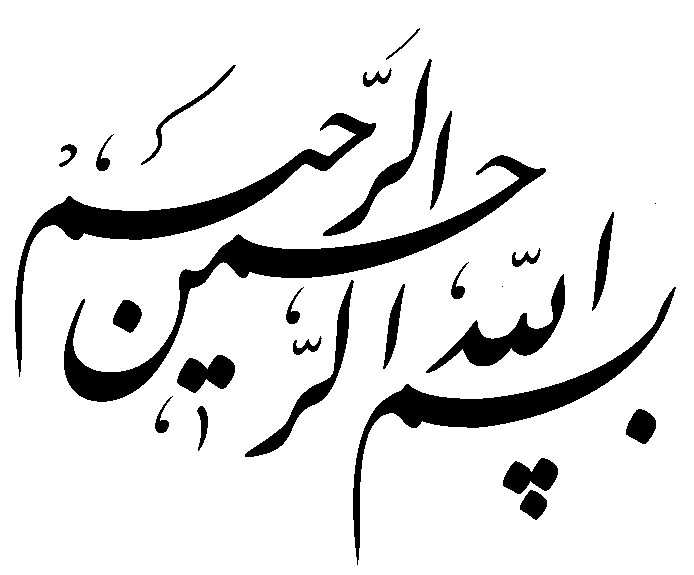
**تحليل نيازمندی‌های غیر کارکردی پلتفرم اينترنت اشياء (مقیاس­پذیری، دسترس­پذیری و امنیت)**

**كد سند:**

**IoT-RA-NonFunc-v1.0**

**تاريخ:**

**15/01/97**



اطلاعات سند

|  |  |
| --- | --- |
| نام پروژه: | طراحي و پياده‌سازي پلتفرم اينترنت اشياء |
| نام سند: | تحليل نيازمندی‌های غیر کارکردی پلتفرم اینترنت اشیا ( مقیاس­پذیری، دسترس­پذیری و امنیت) |
| کد سند: | IoT-RA-NonFunc-v1.0 |
| وضعيت: | نهایی |
| تاريخ انتشار نهايي: | --- |
| نوع طبقه‌بندي سند: | محرمانه |

تاریخچه بازبینی‌ها

|  |  |  |  |
| --- | --- | --- | --- |
| ردیف | نام بازبینی کننده | تاریخ بازبینی | تغييرات |
| 1 | تيم فني | 05/9/96 | تهيه نسخه اوليه بر اساس توافقات جلسه 29/8/96 |
| 2 | تیم فنی | 15/01/97 | ویرایش فنی وادبی |
| 3 |  |  |  |
| 4 |  |  |  |

چکيده

این سند در راستای پوشش فاز 2 پروژه پلتفرم اینترنت اشیا تهیه شده است. در این فاز تحلیل نیازمندی­های کارکردی و غیر کارکردی پلتفرم مد نظر می­باشد. این سند نیازمندی‌های غیرکارکردی پلتفرم اینترنت اشیاء در بخش امنیت، دسترس­پذیری و مقیاس­پذیری را شامل می­شود.

فهرست مطالب

[فصل 1: نيازمندي‌هاي غیرکارکردی 6](#_Toc514707312)

[1-1- دسترس­پذیری 6](#_Toc514707313)

[1-1-1- نیازمندی­های دسترس پذیری 6](#_Toc514707314)

[1-2- مقیاس­پذیری 7](#_Toc514707315)

[1-3- امنیت 7](#_Toc514707316)

[1-3-1- نیازمندی­های امنیت 8](#_Toc514707317)

فهرست جداول

[جدول (1-1) نيازمندي‌هاي دسترس­پذیری 6](#_Toc514707292)

[جدول (1-2) نيازمندي‌هاي مقیاس­پذیری 7](#_Toc514707293)

[جدول (1-3) نيازمندي‌هاي امنیت 8](#_Toc514707294)

1. نيازمندي‌هاي غیرکارکردی
   1. دسترس­پذیری

با توجه به حجم و اهمیت داده جمع­آوری شده در IoT و همچنین ارائه سرویس­های حیاتی در پلتفرم، در دسترس بودن هر دوی این موارد اهمیت فراوانی دارد. شناسایی نیازمندی­های مربوط به دسترس­پذیری در این بخش مورد بررسی قرار گرفته است.

* + 1. نیازمندی­های دسترس پذیری

نيازمندي‌هاي دسترسي پذيري كه مي‌بايست در پياده‌سازي پلتفرم انجام گيرد در ‏جدول (1-1) نشان داده شده است.

نيازمندي‌هاي دسترس­پذیری

| **ردیف** | **کد** | **نیازمندی** | **ملاحظات** |
| --- | --- | --- | --- |
| ۱ | Avl-1 | در صورت خرابی ماژول­های نرم­افزاری، کل پلتفرم تحت تاثیر قرار نگیرد. بازیابی ماژول از کار افتاده به صورت اتوماتیک باشد. | سرویس تا زمان بازیابی قطع خواهد بود. |
| 2 | Avl -2 | از پایگاه داده به صورت آنلاین پشتیبان تهیه گردد. | از Redundant Database Cluster استفاده می­گردد. |
| 3 | Avl -3 | در صورت خرابی ماشین فیزیکی، بازیابی به صورت اتوماتیک صورت پذیرد. | 1. 1- سرویس تا زمان بازیابي قطع مي‌گردد. 2. 2- بازيابي تنها در صورت وجود ماشين فيزيكي mirror قابل انجام است. |

* 1. مقیاس­پذیری

مقیاس­پذیری یا Scalability در ساده­ترین حالت به این معنی است که بتوان از طریق افزایش منابع درخواست­های در حال افزایش به پلتفرم را به صورت کارا پاسخ داد. در پلتفرم IoT به صورت مشخص تعداد زیادی اشیا برای تعداد زیاد کاربران باید فراهم گردد و امکان افزایش درخواست در هر دوی این ابعاد وجود دارد. طراحی معماری و توسعه پلتفرم باید به نحوی باشد که بتواند به افزایش این درخواست­ها پاسخ دهد. ابعاد مختلفی از مقیاس­پذیری قابل بحث می­باشد که دو بعد توسعه افقی (افزودن منابع پردازشی، حافظه­ای و ... به همان منابع قبلی موجود)و عمودی (اضافه کردن منابع جدید به منابع موجود) در آن معمولا بحث می­گردد. نیازمندی­های ذکر شده برای مقیاس­پذیری به شرح زیر است:

نيازمندي‌هاي مقیاس­پذیری

| **ردیف** | **کد** | **نیازمندی** | **ملاحظات** |
| --- | --- | --- | --- |
| ۱ | Sca-1 | سامانه قابلیت پشتیبانی از حداقل 5000 شی را داشته باشد. | بر اساس RFP |
| 2 | Sca -2 | معماری ارائه شده قابلیت مقیاس­پذیری عمودی داشته باشد. |  |
| 3 | Sca -3 | معماری ارائه شده قابلیت مقیاس­پذیری افقی داشته باشد. |  |
| 4 | Sca -4 | مقیاس­پذیری در دو بعد افزایش کاربران و افزایش اشیا حاصل گردد |  |

* 1. امنیت

امنیت در پلتفرم IoT ابعاد مختلفی را در بر می­گیرد که شامل امنیت Applicationها، پروتکل­های ارتباطی و زیرساخت آن می­باشد. در ادامه نیازمندی­های مطرح شده در بخش امنیت پلتفرم مورد بررسی قرار می­گیرد. لازم به ذكر است كه طرح امنيتي كه نحوه پوشش اين نيازمندي‌ها را شرح مي‌دهد در سند جداگانه مربوط به طراحي امنیت سامانه ارائه خواهد گردید.

* + 1. نیازمندی­های امنیت

نيازمندي‌هاي امنیت كه مي‌بايست در پياده‌سازي پلتفرم انجام گيرد در ‏‏جدول (1-3) نشان داده شده است. نيازمندي‌هاي امنيتي را ميتوان در چندين حوزه كلي به شرح زير مورد بررسي قرار داد:

* امنيت ارتباط موجوديتهاي بيرون از پلتفرم با آن

اشياء، برنامه‌هاي كاربردي و قسمتي از UI موجوديتهايي هستند كه بيرون از پلتفرم اجراء شده و به آن متصل مي‌شود. اين موجوديت­ها اولا بايد از پروتكل‌هاي امن براي ارتباط با پلتفرم استفاده كنند ثانيا بايد هويت آنها احراز شود.

* امنيت زيرساخت پلتفرم

پلتفرم بر روي يك زيرساخت نرم‌افزاري اجرا مي‌گردد. اين زيرساخت مي‌بايست امن باشد.

* امنيت اجزای پلتفرم

پلتفرم از اجزای مختلفي تشكيل شده است كه هر يك از آنها سرويسي را ارايه ميكنند. اين اجزا بايد به صورت امن پياده‌سازي شوند.

* امنيت اجراي كد كاربر

يكي از نيازمندي‌هاي مد نظر در پلتفرم امكان اجراي كد كاربر است، اين قابليت نبايد امنيت خود پلتفرم را به مخاطره بياندازد.

* امنيت شبكه و زيرساخت فيزيكي

علاوه بر نيازمندي‌هاي فوق كه امنيت پلتفرم و ارتباط آن با ساير موجوديت‌ها را تامين مي‌كند، شبكه و زيرساخت فيزيكي كه پلتفرم در آن نصب و راه‌اندازي و بهره‌برداري مي‌شود نيز بايد امن باشد. پياده‌سازي اين مورد خارج از محدود اين پروژه است و در حد توصیه موارد مربوطه ارائه خواهد گردید، بنابراين موردي براي آن در جدول زير ذكر نشده است.

نيازمندي‌هاي امنیت

| **ردیف** | **کد** | **نیازمندی** | **ملاحظات** |
| --- | --- | --- | --- |
| 1 | Sec-1 | ارتباط UI از طریق پروتکل­های امن صورت پذیرد. |  |
| 2 | Sec-2 | پروتکل­های ارتباطی برنامه­کاربردی امن گردد:   * امن سازی Rest به وسیله‌ی jwt یا oAuth   امن سازی MQTT ( TLS/SSL – App level security) | از پروتكلهاي موجود براي اين منظور استفاده خواهد شد. |
| 3 | Sec-3 | از پروتکل­های امن براي اتصال به اشیا استفاده گردد. | قابليت‌هاي امنيتي پروتكل‌هاي مورد استفاده فعال خواهد شد. |
| 4 | Sec-4 | احراز هویت در پروتکل­های ارتباطی برنامه­های کاربردی و واسط کاربری انجام پذیرد. |  |
| 5 | Sec-5 | قابليت‌هاي امنيتي سيستم عامل بايد فعال شوند. |  |
| 6 | Sec-6 | قابليت‌هاي امنيتي زيرساخت ميكرو سرويس بايد فعال شوند. |  |
| 7 | Sec-7 | سرويس‌هاي ارايه دهنده API به UI و برنامه‌هاي كاربردي بايد به صورت امن پياده‌سازي شود. |  |
| 8 | Sec-8 | سرويس‌هاي دريافت داده از اشياء بايد به صورت امن پياده‌سازي شود. |  |
| 9 | Sec-9 | واسط كاربري بايد به صورت امن پياده‌سازي گردد. |  |
| 10 | Sec-10 | قابليت‌هاي امنيتي پايگاه‌‌داده بايد فعال گردد. |  |
| 11 | Sec-11 | كد‌هاي مخرب كاربران نبايد امنيت پلتفرم را تحت تاثير قرار دهد. براي اين منظور   * منابع مورد استفاده براي اجراي آنها بايد محدود باشد.   دسترسي به برخي منابع براي اين كدها محدود باشد. | جزييات اين موارد در فاز طراحي مشخص خواهد شد. |