پژوهشگاه فضایی ایران

ISRC

مرکز تحقیقات فضایی

عنوان اختصاری پروژه: اینترنت اشیاء کشاورزی
کد پروژه: CNS**۹۹۹۷-۰۱**
کد فعالیت: CNS**۹۹۹۷-۰۱-۰۷**

تحلیل نیازمندی‌های غیر کارکردی پلتفرم اینترنت اشیاء (مقیاس‌پذیری، دسترس‌پذیری و امنیت)

کد سند: MSRI-CNS**۹۹۹۷-۰۱**/R-**۰۷/۰۳**
شماره ویرایش: ۱/۱
طبقه‌بندی: عادی
تاریخ: ۹۷/۰۴/۱۶

تعداد کل صفحات: ۱۸ صفحه

(با احتساب برگ روی جلد)

استفاده از این سند صرفا توسط گیرندگان مجاز است.

بسم الله الرحمن الرحيم

شناسنامه سند

۱- مشخصات پروژه

عنوان کامل پروژه	**انجام مطالعات امکانسنجی و پیاده سازی ایده اینترنت اشیاء در حوزه کشاورزی**			**مدیر پروژه**	-
کد پروژه	CNS**۹۹۹۷-۰۱**	**پژوهشکده (حوزه) مجری**	مرکز تحقیقات فضایی	**تاریخ شروع پروژه**	۹۵/۰۲/۰۱
کد فعالیت	CNS**۹۹۹۷-۰۱-۰۷**			**تاریخ خاتمه پروژه**	۹۵/۰۹/۰۱

۲- مشخصات سند

عنوان سند	تحلیل نیازمندی‌های غیر کارکردی پلتفرم اینترنت اشیاء (مقیاس‌پذیری، دسترس‌پذیری و امنیت)			**تعداد صفحات**	
طبقه‌بندی سند	عادی	**کد سند**	MSRI-CNS**۹۹۹۷-۰۱**/R-**۰۷/۰۳**	**کل سند**	۱۸
ویرایش	۱/۱	**تاریخ ویرایش**	**۹۷/۰۴/۱۶**	**پیوست‌ها**	**۱۱**

۳- جدول تهیه، تایید و تصویب در پژوهشکده (حوزه) مجری

	سمت*	**نام و نام‌خانوادگی**	**امضا**	**تاریخ**
تهیه‌کننده(گان)	**رییس بخش طراحی و پیاده سازی نرم افزار**			
تاییدکننده(گان)	**رییس اداره برنامه ریزی**			
تصویب‌کننده	**رییس مرکز**			

*** برای مواردی که مجری، حوزه دیگری غیر از پژوهشکده است، مثل مراکز یا گروه‌های پژوهشی مستقل و ... از سمت‌های معادل بر اساس نظر رییس حوزه استفاده شود.**

شناسنامه سند (ادامه)

۴- جدول تایید و تصویب در پژوهشگاه

	سمت	نام و نام‌خانوادگی	امضا	تاریخ
تاییدکننده(گان)	مدیران مرکز طراحی و توسعه سامانه‌های فضایی یا مدیر پژوهش و فناوری (برحسب مورد)			
	سایر افراد (مانند معاون تضمین کیفیت، بهره‌بردار و ... براساس قرارداد یا نظر تصویب‌کننده و مدیریت کنترل پروژه)			
تصویب‌کننده	رییس مرکز طراحی و توسعه سامانه‌های فضایی یا معاون پژوهش و فناوری(برحسب مورد)			

۵- جدول توزیع نسخ (گیرندگان)

عنوان واحد	توزیع	عنوان واحد	توزیع
ریاست پژوهشگاه فضایی ایران		مدیریت راهبرد و طراحی ماموریت	
دفتر ریاست، روابط عمومی و امور بین الملل		مدیریت مهندسی سامانه‌های فضایی	
مدیریت حراست		مدیریت آزمون و عملیات میدان	
اداره امور حقوقی		**معاونت اجرایی**	
مدیریت نظارت و ارزیابی و پاسخگویی به شکایات		مدیریت توسعه منابع انسانی	
مدیریت بازرگانی خارجی		مدیریت پشتیبانی	
مدیریت طرح و برنامه	●	مدیریت امور مالی	
معاونت پژوهش و فناوری		اداره تشکیلات و بهبود روش‌ها	
مدیریت آموزش و تحصیلات تکمیلی		**سازمان فضایی ایران**	
مدیریت پژوهش و فناوری	✓	**پژوهشکده سامانه‌های حمل‌ونقل فضایی**	
مدیریت دانش		**پژوهشکده سامانه‌های ماهواره**	
معاونت تضمین کیفیت و ایمنی		**پژوهشکده مکانیک**	
مدیریت مهندسی تضمین کیفیت		**پژوهشکده مواد و انرژی**	
مدیریت کالیبراسیون و استاندارد		**پژوهشکده رانشگرهای فضایی**	
مدیریت ایمنی و محیط زیست		**مرکز تحقیقات فضایی**	✓
مرکز طراحی و توسعه سامانه‌های فضایی			
سایر گیرندگان:			

***توزیع نسخ بر اساس علامت‌های زیر انجام می‌شود:**

✓: سند برای این واحدها ارسال می‌شود.

●: سند برای این واحدها ارسال نمی‌شود و صرفا اطلاع‌رسانی می‌شود.

۶- تایید مرکز اسناد

مدیریت دانش (مرکز اسناد) پژوهشکده مجری
نام و نام‌خانوادگی: .....
تاریخ: .....
مهر و امضا

مدیریت دانش (مرکز اسناد) پژوهشگاه فضایی ایران
نام و نام‌خانوادگی: .....
تاریخ: .....
مهر و امضا

شناسنامه سند (ادامه)

۷- جدول مشخصات و شرح وظایف دست‌اندرکاران تدوین سند*

ردیف	نام و نام‌خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	مرتبه علمی**	محل کار	شرح وظایف	درصد مشارکت
۱	دانشگاه امیرکبیر				دانشگاه امیرکبیر		۱۰۰
۲							
۳							
۴							
۵							
۶							
۷							
۸							
۹							
جمع							**۱۰۰**

*منظور کلیه افرادی است که در انجام فعالیت‌های مرتبط با این سند نقش اصلی داشته‌اند.

**برای اعضای هیات علمی از عناوین مربوط (استاد، دانشیار، استادیار، مربی) و برای دیگر پژوهشگران از عنوان کارشناس استفاده شود.

۸- دیگر همکاران تدوین سند*

ردیف	نام و نام‌خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	مرتبه علمی	محل کار	نقش

* منظور کسانی است که ضمن مطالعه سند، نظرات قابل توجهی را در خصوص سند ارائه کرده‌اند. ویراستاران ادبی نیز در این جدول ذکر می‌شوند.

شناسنامه سند (ادامه)

۹- جدول مشخصات ناظر(ان)

ردیف	نام و نام‌خانوادگی	آخرین مدرک	رشته	مرتبه علمی	محل کار	توضیحات
۱	احسان پناهی	فوق لیسانس		کارشناس	مرکز تحقیقات فضایی	

۱۰- جدول سوابق ویرایش و تغییرات

ویرایش	تاریخ	شرح تغییرات	علت/مرجع تغییر	واحد تهیه‌کننده مسئول
۱/۱	۹۶/۰۴/۱۶	نگارش سند	-	-

چکیده

گزارش حاضر حاوی سند دریافتی از دانشگاه امیرکبیر (پیمانکار پژوهشگاه فضایی ایران در قرارداد "طراحی و پیاده سازی پلتفرم اینترنت اشیاء) با عنوان "تحلیل نیازمندی‌های غیر کارکردی پلتفرم اینترنت اشیاء (مقیاس‌پذیری، دسترس‌پذیری و امنیت)" می باشد.

واژه‌های کلیدی:

اینترنت اشیا، پلتفرم، کشاورزی هوشمند

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

آزمایشگاه اینترنت اشیاء

گروه پلتفرم

عنوان سند:

تحلیل نیازمندی‌های غیر کارکردی پلتفرم اینترنت اشیاء (مقیاس‌پذیری، دسترس‌پذیری و امنیت)

کد سند:

IoT-RA-NonFunc-v۱,۰

تاریخ:

۹۷/۰۱/۱۵

کلیه حقوق هر نوع استفاده از این سند نزد آزمایشگاه اینترنت اشیاء دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر محفوظ می‌باشد.

بسم الله الرحمن الرحیم

اطلاعات سند

نام پروژه:	طراحی و پیاده‌سازی پلتفرم اینترنت اشیاء
نام سند:	تحلیل نیازمندی‌های غیر کارکردی پلتفرم اینترنت اشیا (مقیاس‌پذیری، دسترس‌پذیری و امنیت)
کد سند:	IoT-RA-NonFunc-v۱,۰
وضعیت:	نهایی
تاریخ انتشار نهایی:	---
نوع طبقه‌بندی سند:	محرمانه

تاریخچه بازبینی‌ها

ردیف	نام بازبینی کننده	تاریخ بازبینی	تغییرات
۱	تیم فنی	۹۶/۹/۰۵	تهیه نسخه اولیه بر اساس توافقات جلسه ۹۶/۸/۲۹
۲	تیم فنی	۹۷/۰۱/۱۵	ویرایش فنی وادبی
۳			
۴			

چکیده

این سند در راستای پوشش فاز ۲ 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 ۱: نیازمندی‌های غیرکارکردی ٦
۱-۱- دسترس‌پذیری ۶
۱-۱-۱- نیازمندی‌های دسترس پذیری ۶
۱-۲- مقیاس‌پذیری ۷
۱-۳- امنیت ۷
۱-۳-۱- نیازمندی‌های امنیت ۸

فهرست جداول

جدول (۱-۱) نیازمندی‌های دسترس‌پذیری ۶
جدول (۱-۲) نیازمندی‌های مقیاس‌پذیری ۷
جدول (۱-۳) نیازمندی‌های امنیت ۸

فصل ۱:
نیازمندی‌های غیرکارکردی

۱-۱- 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.

۱-۱-۱- نیازمندی‌های دسترس پذیری

نیازمندی‌های دسترسی پذیری که می‌بایست در پیاده‌سازی پلتفرم انجام گیرد در جدول (۱-۱) نشان داده شده است.

جدول (۱-۱) نیازمندی‌های دسترس‌پذیری

ردیف	کد	نیازمندی	ملاحظات
۱	Avl-۱	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.
۲	Avl -۲	از پایگاه داده به صورت آنلاین پشتیبان تهیه گردد.	از Redundant Database Cluster استفاده می‌گردد.
۳	Avl -۳	در صورت خرابی ماشین فیزیکی، بازیابی به صورت اتوماتیک صورت پذیرد.	۱- سرویس تا زمان بازیابی قطع می‌گردد.

ردیف	کد	نیازمندی	ملاحظات
			۲- بازیابی تنها در صورت وجود ماشین فیزیکی mirror قابل انجام است.

۱-۲- مقیاس‌پذیری

مقیاس‌پذیری یا Scalability در ساده‌ترین حالت به این معنی است که بتوان از طریق افزایش منابع درخواست-های 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:

جدول (۱-۲) نیازمندی‌های مقیاس‌پذیری

ردیف	کد	نیازمندی	ملاحظات
۱	Sca-۱	سامانه قابلیت پشتیبانی از حداقل ۵۰۰۰ شی را داشته باشد.	بر اساس RFP
۲	Sca -۲	معماری ارائه شده قابلیت مقیاس‌پذیری عمودی داشته باشد.	
۳	Sca -۳	معماری ارائه شده قابلیت مقیاس‌پذیری افقی داشته باشد.	
۴	Sca -۴	مقیاس‌پذیری در دو بعد افزایش کاربران و افزایش اشیا حاصل گردد	

۱-۳- 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 ذکر است که طرح امنیتی که نحوه پوشش این نیازمندی‌ها را شرح می‌دهد در سند جداگانه مربوط به طراحی امنیت سامانه ارائه خواهد گردید.

۱-۳-۱- نیازمندی‌های امنیت

نیازمندی‌های امنیت که می‌بایست در پیاده‌سازی پلتفرم انجام گیرد در جدول (۱-۳) نشان داده شده است. نیازمندی‌های امنیتی را میتوان در چندین حوزه کلی به شرح زیر مورد بررسی قرار داد:

- امنیت ارتباط موجودیتهای بیرون از پلتفرم با آن

اشیاء، برنامه‌های کاربردی و قسمتی از UI موجودیتهایی هستند که بیرون از پلتفرم اجراء شده و به آن متصل می‌شود. این موجودیت‌ها اولا باید از پروتکل‌های امن برای ارتباط با پلتفرم استفاده کنند ثانیا باید هویت آنها احراز شود.

- امنیت زیرساخت پلتفرم

پلتفرم بر روی یک زیرساخت نرم‌افزاری اجرا می‌گردد. این زیرساخت می‌بایست امن باشد.

- امنیت اجزای پلتفرم

پلتفرم از اجزای مختلفی تشکیل شده است که هر یک از آنها سرویسی را ارایه میکنند. این اجزا باید به صورت امن پیاده‌سازی شوند.

- امنیت اجرای کد کاربر

یکی از نیازمندی‌های مد نظر در پلتفرم امکان اجرای کد کاربر است، این قابلیت نباید امنیت خود پلتفرم را به مخاطره بیاندازد.

- امنیت شبکه و زیرساخت فیزیکی

علاوه بر نیازمندی‌های فوق که امنیت پلتفرم و ارتباط آن با سایر موجودیت‌ها را تامین می‌کند، شبکه و زیرساخت فیزیکی که پلتفرم در آن نصب و راه‌اندازی و بهره‌برداری می‌شود نیز باید امن باشد. پیاده‌سازی این مورد خارج از محدود این پروژه است و در حد توصیه موارد مربوطه ارائه خواهد گردید، بنابراین موردی برای آن در جدول زیر ذکر نشده است.

جدول (۱-۳) نیازمندی‌های امنیت

ردیف	کد	نیازمندی	ملاحظات
۱	Sec-۱	ارتباط UI از طریق پروتکل‌های امن صورت پذیرد.	
۲	Sec-۲	پروتکل‌های ارتباطی برنامه‌کاربردی امن گردد: • امن سازی Rest به وسیله‌ی jwt یا oAuth امن سازی MQTT (App level security – TLS/SSL)	از پروتکلهای موجود برای این منظور استفاده خواهد شد.
۳	Sec-۳	از پروتکل‌های امن برای اتصال به اشیا استفاده گردد.	قابلیت‌های امنیتی پروتکل‌های مورد استفاده فعال خواهد شد.

ردیف	کد	نیازمندی	ملاحظات
۴	Sec-۴	احراز هویت در پروتکل‌های ارتباطی برنامه‌های کاربردی و واسط کاربری انجام پذیرد.	
۵	Sec-۵	قابلیت‌های امنیتی سیستم عامل باید فعال شوند.	
۶	Sec-۶	قابلیت‌های امنیتی زیرساخت میکرو سرویس باید فعال شوند.	
۷	Sec-۷	سرویس‌های ارایه دهنده API به UI و برنامه‌های کاربردی باید به صورت امن پیاده‌سازی شود.	
۸	Sec-۸	سرویس‌های دریافت داده از اشیاء باید به صورت امن پیاده‌سازی شود.	
۹	Sec-۹	واسط کاربری باید به صورت امن پیاده‌سازی گردد.	
۱۰	Sec-۱۰	قابلیت‌های امنیتی پایگاه‌داده باید فعال گردد.	
۱۱	Sec-۱۱	کدهای مخرب کاربران نباید امنیت پلتفرم را تحت تاثیر قرار دهد. برای این منظور • منابع مورد استفاده برای اجرای آنها باید محدود باشد. دسترسی به برخی منابع برای این کدها محدود باشد.	جزییات این موارد در فاز طراحی مشخص خواهد شد.