حریم خصوصی در اینترنت اشیا :

مدل و چارچوب حفاظتی

چکیده

یک شکل جدیدی از محاسبات ،شکل تکامل یافته ی تعداد گسترده ای از مجموعه ی متنوع سیستم های محاسباتی متعارف است که شامل ، سنسورها ،دستگاه ها ،تجهیزات ،نرم افزار و اطلاعات خدمات و برنامه میشود.این شکل جدید از محیط محاسباتی به نام اینترنت اشیا یا (IOT) شناخته میشود.پذیرش اینترنت اشیا سریع است و اشیا در حال تبدیل به عضو جدایی ناپذیر از زندگی روزمره مردم و همچنین عناصر ضروری در فعالیت های روزمره کسب و کار و فرآیندها هستند.ویژگی های گسترده محیطی اشیا ،نگرانی های حفظ حریم خصوصی را به عنوان اشیایی مستقل به همراه درجه ای از اختیار در به اشتراک گذاشتن توانایی های خود ،و دانش به انجام رساندن توانایی های فردی و اجتماعی خود،بر انگیخته است.به این ترتیب حفظ حریم خصوصی مرکزی میشود و یک جنبه محاسباتی از اشیا را به ارث میبرد.کار ارایه شده در اینجا بر اساس مدل اینترنت اشیا به عنوان یک سیستم توزیعی تعاونی(CDS)است.این یک رویکرد نوین از تجزیه و تحلیل و مدل سازی مفاهیم و نگرانی های حریم خصوصی است.حفاظت از حریم خصوصی به عنوان یک فرم از مدیریت "حساسیت اطلاعات" در سطح تعامل ایجاد شده است.چارچوب مدیریت حفظ حریم خصوصی برای سیستم توزیع تعاونی در سطح تعامل ارایه شده است.برنامه استفاده از چارچوب توسط گسترش قرارداد پروتکل شبکه ،برای حمایت از حفظ حریم خصوصی سیستم توزیع تعاونی، نشان داده شده است.

معرفی

اینترنت اشیا در حال تبدیل به یک محیط رقابتی جدید با بهم پیوستن اشیا مانند ،خدمات اطلاعاتی و دستگاه ها، تجهیزات و سنسورها با نرم افزار است. آنها قادر به برقراری ارتباط با یکدیگر از طریق اینترنت هستند. رشد آینده اینترنت اشیا بر پایه برنامه ها، بسیار عظیم پیش بینی شده است. یکپارچه سازی شبکه اجتماعی و تکنولوی محاسبات همه گیر در اینترنت اشیا مردم را به صورت فردی و گروهی قادر به ارتباط با محیط میکند[1] .آسایشی که در نوآوری تکنولوژی اینترنت اشیا همراه با حفظ حریم شخصی آزموده شده ، همراه با هزینه ی بسیاری بوده است [2،3].برای مثال، فرآیند سنسور اطلاعات در خانه ای که راهرو و درهایش مجهز به منبع نور و سنسورهای مغناطیسی است میتواند موجب به نمایش گذاشتن ساختمان که طرح آن ممکن است دارای هدف سوء باشد ،میشود. در مثالی دیگر ،بعد از این که آنها در مغازه حضور پیدا میکنند و سنسور ویدئو از آنها عکس هایی تهیه میکند ،پیامی در صفحه فیسبوک مشتری نشان داده میشود. سرویس تشخیص هویت نام آنها ،و سامانه بازشناسی با امواج رادیویی(RFID) مکان مغازه را ضمیمه میکند. در این میان نه تنها مردم ردیابی میشوند بلکه مکان آنها نیز در شبکه آنها به اشتراک گذاشته میشود. علی رغم اشتغال در مکانیزم حفظ حریم شخصی ،مانند اسم مستعار ،تجارت ،رویکرد مبتنی بر وکالت ، و قرار دادن بیشتر محدودیت های عمیق روی تشخیص و استخراج داده ،حفظ حریم شخصی هنوز در اینترنت اشیا درگیر چالش بزرگی است.بعضی ازین مدل ها تنظیمات خاصی را روی محیط اعمال میکنند.بعضی دیگر فقط آدرس ویژگی های اشیا را نمی دهند بلکه اطلاعات جمع میکنند.همچنین بعضی مدل های حفاظت حریم شخصی وفادار به بعهده گیری اشیا مورد اعتماد در محیط هستند.

نگرانی حفظ حریم شخصی ،سیستم های محاسباتی است که دارای محاسبات غیر متمرکز هستند.برای مقابله ،حفظ حریم خصوصی باید به عنوان بخش جدایی ناپذیر از سطح محاسبات ،ضبط شود.این به رفتار حفظ حریم شخصی مانند یک هدف ریاضی و ترکیب آن به عنوان یک عامل کیفیت برای مسائلی که محاسبه شده ،نیاز دارد.به عنوان نتیجه ،حل و فصل حریم خصوصی در اینترنت اشیا ،مستلزم مدل سازی آن به عنوان زمینه محاسباتی است.این مقاله اینترنت اشیا را مانند سیستم های توزیعی تعاونی شده (CDS) ،به عنوان زمینه ی محاسبات که در آن نهاد ها

مستقل و خود مختار هستند ،مدلسازی میکند.انتظار میرود که نهادها ،میتوانند برخی از درجه های قدرت در تبادل اطلاعات و قابلیت ،با دیگران را داشته باشند.تعامل از طریق تبادل پیام صورت میگیرد.تلاش ما در تجزیه و تحلیل حریم خصوصی در سیستم های توزیعی تعاونی ،در گسترش دادن یک مدل که حفظ حریم شخصی را مانند یک مفهوم محاسباتی نشان میدهد ،نتیجه داده است و به عنوان یک ابزار تحلیلی که برای ارزیابی دولت از حفظ حریم خصوصی در تنظیمات مختلف تعاملات در سیستم های توزیعی تعاونی استفاده میشود.ما یک تعامل مبنی بر چارچوب حفظ حریم خصوصی که اشیا در اینترنت اشیا ،وابسته به حفاظت از حریم خصوصی که در زمینه محاسبات ضبط شده اند را پیشنهاد میدهیم.

دستیابی های اخیر برای حفظ حریم خصوصی در محیط های نا همگن مانند اینترنت اشیا میتواند به دو دسته اصلی ،طبقه بندی شود :رویکرد های مبتنی بر قانون و رویکرد های مبتنی بر معماری.مدل های راه حل حفظ حریم خصوصی از قانون مبتنی بر مدل های معمولی که برای محیط های بسته طراحی شده اند ،جدا شده است.این رویکرد ها به طور عمده ،در اعمال قوانین بر روی اطلاعات به اشتراک گذاشته شده ،متمرکز است.به دلیل فرض باز بودن محیط در اینترنت اشیا ،روش های مبتنی بر قانون [9] کافی نیست.در بین راه حل های حفظ حریم شخصی مبتنی بر معماری ،تکنیک های ناشناسی هستند مانند [4,11]،مکانیزم تجارت ابزار حفظ حریم شخصی [5,12]،تبادل اجتماعی و قانون مبنی بر حفاظت حریم شخصی [6].به هر حال در این زمینه ،تکنیک های نا شناس ،محدود به تنظیمات خاص شامل شرکت کنندگان ،جمع آوری کننده اطلاعات و حریفی که باعث تلاش برای جمع آوری اطلاعات فردی از جمع آوری کننده اطلاعات میشود ،وجود دارد.در این زمینه فرض بر این است که ،جمع آوری کننده اطلاعات یک طرف مورد اعتماد است.این مکانیزم ها در جهت محافظت از اطلاعات حساس ،مانند مشارکت اشیا در فرآیند جمع آوری اطلاعات طراحی شده است.آن ها به افشای اطلاعات جمع شده که نسبت داده شده به اشیا ،نمی پردازند [4].ابزار تجارت سودمند مبتنی بر ارزیابی اطلاعات بدست آمده از رد و بدل اطلاعات است.

این مقاله معماری بر پایه ی حفظ حریم شخصی را پیشنهاد میدهد.بقیه مقاله تهیه شده به شرح زیر است.بخش 2 ،بعضی از ویژگی های محیطی اینترنت اشیا و مدل های آن مانند سیستم های توزیعی تعاونی را بیان میکند.بخش 3

مدلی را برای حریم خصوصی در مدل سیستم های توزیعی تعاونی ارائه میدهد.بخش 3 ،چارچوبی را برای مدیریت حفاظت از حریم خصوصی در سطح تعاملی برای سیستم های توزیعی تعاونی مبتنی بر اینترنت اشیا ،شرح میدهد.در نهایت کار در بخش 5 گنجانده شده است.

2. اینترنت اشیا:مشخصات و مدل

در این کار ،عنصر اصلی اینترنت اشیا ،اشیایی که مجهز به فرآیند های محاسباتی دیجیتال و قابلیت های ارتباطی مبتنی بر اینترنت ،هستند. اشیا قابلیت تبادل اطلاعات را بین دیگر اشیا ،در تلاش برای همکاری برای بدست آوردن اهداف فردی و اجتماعی ،دارند.رسیدن به اهداف اشیا ممکن است فراتر از توانایی آنها باشد ،بنابراین برای رسیدن به آنها ممکن است با دیگران هماهنگ شوند.اینترنت اشیا به طور طبیعی ،به عنوان یک محیط باز که در آن با انواع متفاوت طراحی ،اهداف و رفتار کسب و کار ،میتوانند به محیط بپیوندند یا در هر زمانی آن را ترک کنند.این ،به اندازه کافی مدل اینترنت اشیا را به عنوان یک سیستم توزیعی تعاونی هدایت میکند ،که در آن نهاد های اشیا هوشمند ، توانایی انجام قابلیت هارا با قابلیت هماهنگی فعالیت های خود با دیگران برای رسیدن به اهداف فردی یا جمعی ،را دارند.بنابر این اشیا هوشمند با دانش ناقص میتوانند خود مختار و به نفع خود باشند.در این زمینه ،اشیا هوشمند نشان دهنده اشیائی است که قادر به اشتراک گذاری اطلاعات و تصمیم گیری بر اساس اهداف مورد علاقه خود است.

اینترنت اشیا به طور روز افزونی جدایی ناپذیر از کسب و کار روزانه زندگی مردم است به طوری که ،ممکن است اطلاعات به عنوان حساسیت بین اشیا هوشمند و محیط ،در نظر گرفته شود.برای ارائه خدمات ،اطلاعات ممکن است برای جمع آوری یا انجام فرآیند ،با اشیای هوشمند بین محیط تعویض یا رد وبدل شود.این ممکن است به نگرانی حریم خصوصی تحمیل شود.به عنوان مثال ،حسگر های مغناطیسی میتوانند از طریق اینترنت ،توانا ساز باز کننده در را فعال کنند.به هر حال ،بنا به دلایل امنیتی آنهارا به حسگر های ویدیویی برای اجازه مردم هنگام دخول ،مجهزکرده اند.استفاده از برنامه های تشخیص چهره روی فیلم ترکیب شده با فرکانس حضور مردم در خانه ،ممکن است منجر

به شناسایی اعضای خانواده از جمله کودکان شود.استفاده از نرم افزار تشخیص چهره ی فیسبوک ،باعث میشود صفحات فیسبوک و مدرسه ای که آنها میروند را پیدا کند [13]،[14].

3.حریم خصوصی: مفاهیم ،تجزیه و تحلیل و مدل

تمرکز در این بخش بر پایه تجزیه و تحلیل جنبه های اصلی نگرانی های حریم خصوصی و مفاهیمی که برای گسترش چارچوب حفاظت حریم شخصی ،ضروری است.به اشتراک گذاری اطلاعات هر زمان که بین اشیا هوشمند و اینترنت اشیا تعاملی صورت گیرد ،انجام میشود.تعامل از طریق ارتباط مبتنی بر پیام ،تحویل داده میشود.این پیام ها حاوی اطلاعاتی هستند که ممکن است نگرانی های حریم خصوصی ،مانند اشیای هوشمندی که علاقه ای به اشتراک گذاشتن اطلاعات حساس با بقیه ندارند ،را بر می انگیزند.برای هر گونه از اطلاعات یا حالتی از اشیا هوشمند که داده شده ،یک مرز برای قرار گرفتن اطلاعات به اشتراک گذاشته شده ی غیر مهم وجود دارد.این نشان میدهد تعریف ما از حریم خصوصی ،مانند حالتی از مرز قرار گرفتن بین اطلاعات اشیای هوشمند و دنیای بیرون است.در سیستم های توزیعی تعاملی ،اینترنت اشیا بر اساس ویژگی های اشیای هوشمند مدل سازی شده است. $W= \{ e_1 \dots e_n\}$ در زمینه مدیریت اطلاعات ،اشیا میتوانند به عنوان عملیات و اطلاعات مدلسازی شوند.

$$,1\leq i \leq N \quad I_i \equiv \{I_{i,1} \dots\dots I_{i,k} \dots\dots I_{i,M}\} \quad 1\leq i \leq N \quad 1\leq k \leq M, e_{i=<o_{i,I_i}>}$$

$$\dots, O_{i,w} \dots, O_{i,W}\} \, , \, 1\leq i \leq N \, ,1\leq w \leq W O_i \equiv \{O_{i,1},$$

در این زمینه ،اطلاعاتی که در محدوده جریان میابد ،غیر حساس در نظر گرفته شده ،اما به محض اینکه خارج از محدوده قرار گیرد ،حساس تلقی میشود.به عنوان مثال ،در برنامه های خانه هوشمند که استفاده از اینترنت اشیا را توسعه میدهند ،الگوی مصرف انرژی از هر اتاق ،توسط حسگر هایی که از طریق برنامه در حال اجرا روی تلفن همراه میتوانند با خانه ارتباط برقرار کنند ،جمع آوری میشوند.با این مرز در معرض قرار گرفتن این اطلاعات ،شامل شرکت های ارائه دهنده قدرت نیست.این اطلاعات میتواند برای تشخیص الگوی حضور صاحب خانه در خانه توسط ضبط

کردن کمترین زمان حضور صاحب خانه در خانه که شامل اطلاعات مهمی برای صاحب خانه است.اجازه بدید که $E_{i,k}$در معرض محدوده ای که توسط اینترنت اشیا طراحی شده اند ،قرار گیرد.

$$\text{for } I_{i,k} : E_{i,k} \equiv \{e_{t+1}, \ldots\ldots e_{t+r}\}\ 1 \leq r, t \leq N\ \mathrm{C}\ (e_{i,k}, \mathrm{W}) e_i$$

بر این اساس ،اطلاعات حساس مربوط به اطلاعات به اشتراک گذاشته با اشیا هوشمند ،است.اگر متعلق به معرض قرار گرفتن به محدوده نباشد ،اطلاعات حساس میشود.همچنین ،به اشتراک گذاشتن محتویات اطلاعات حریم خصوصی ،فرآیندی از تبادل اطلاعات صریح و روشن در معرض محدودیت $E_{i,k}$است.

اطلاعات میتواند به طور ضمنی نمایش داده شود."اطلاعات ضمنی" را میتوان با عملیات تبدیل به اطلاعات صریح ودقیق تبدیل کرد.$O(I^{x1}, I^{aux})$

دستکاری اطلاعات صریح I^{x1} ،توسط عملیات پردازش ،تبدیل به فرم اطلاعات ضمنی I^{x2}،که از طریق اجرای عملیات به این صورت نشان داده میشود :

$$(I^{x1}, I^{aux}, I^{x2})\bar{\bar{O}}$$

عملیات ممکن است از اطلاعات کمکی I^{aux}که توسط دارنده آن منتشر نمیشود ،استفاده کند.

اگرچه اشیای هوشمند میتوانند از اطلاعات صریح خود حفاظت کنند ،اما وقتی اطلاعات ضمنی تبدیل به اطلاعات صریح میشود ،میتواند تبدیل به یک نگرانی شود.انتشار اطلاعات میتواند توسط عملیاتی که در آن یکی از قابلیت های آن عملیات تبادل اطلاعات بین اشیا هوشمند است ،مدلسازی شود.

اشتراک گذاری اطلاعات توسط اشیا هوشمندی که دارای عملیاتی هستند که میتوانند اطلاعات مربوط ضمنی را به اطلاعات صریح تبدیل کنند ،آشکار سازی نامیده میشود.این نشان میدهد که افشای اطلاعات غیر حساس صریح و روشن ،میتواند معادل افشای اطلاعات حساس ضمنی باشد.

یکی از چالش های اصلی مدیریت حفاظت از حریم خصوصی ،مقابله با دانش ناقص است.در این زمینه برای اشیا هوشمند رسیدن به دانشی در مورد اشیای هوشمندی که ممکن است تبادل اطلاعات داشته باشد ،ضروری است.میتواند برای بازیابی دلیل افشای اطلاعات بازیابی شود.برای مقابله با این موضوع ،ما عملیات مجاز $O_j^{i,k}$که

مجموعه ای از عملیات متعلق به O_j که e_i برای استفاده آن روی $I_{j,k}$توافق شده است را معرفی میکنیم.به عنوان مثال ،این میتواند با استفاده از قرار داد های حقوقی بین خدمات وبسایت ها اجرا شود.در حالت ایده آل ،این توافقات شامل عملیاتی است که مجاز به اعمال روی اطلاعات به اشتراک گذاشته شده است.متعهد نبودن به توافق بین اشیا هوشمند برای اجرای عملیات غیر مجاز $\hat{O}_{j,t}^{i,k}$ ،"نقض حریم خصوصی" در نظر گرفته شده است.

$$\equiv \{ \hat{O}_{j,1}^{i,k} ,\dots, \hat{O}_{j,t}^{i,k} ,\dots, \hat{O}_{j,T}^{i,k} \} , 1 \leq t \leq T \hat{O}_{j}^{i,k}$$

$$= \cup_{k=1}^{m} (\emptyset, \hat{O}_{j}^{i,k}) \hat{O}_{j}^{i}$$

اشاره دارد به تمام عملیات های غیر مجاز برای مجموعه ای از اطلاعات.

$$= \cup_{\forall s \in (S, PS(S))}^{|PS(S)|} (\emptyset, \hat{O}_{j}^{S}) \hat{O}_{j}^{s}$$

$\downarrow \hat{O}_{j,w}^{i,k}$ اجازه انجام به $\hat{o}_{j,w}^{i,k}$ را نمیدهد.$\theta_{i,j}^{i,k} \equiv \forall w \downarrow \hat{O}_{j,w}^{i,k}$ به عنوان توافق بین e_i و e_j تلقی میشود.

بر این اساس نقض حریم خصوصی می شود :

$$\text{PV}(\quad e_i, I_{i,k}, \hat{O}_{j,}^{i,k}, \theta_{i,j}^{i,k}) \equiv \exists \, w \mid \theta_{i,j}^{i,k} \wedge [\, \hat{\hat{\bar{O}}}_{j,w}^{i,k}(I_{i,k})]$$

در حال حاضر ، $\bar{\bar{O}}(\widetilde{I^{x1}}, I^{aux})$ ناتوانی اشیا هوشمند برای انجام عملیات های غیر مجاز با جلوگیری یا خنثی سازی عملیات ،را نشان میدهد." حفاظت از حریم خصوصی " میتواند به عنوان مکانیزم اجرایی برای جلوگیری و یا خنثی کردن استفاده از عملیات های غیر مجازاطلاعات به اشتراک گذاشته شود.

$$\widehat{\widetilde{O_{j,w}^{t}}} \quad \text{PP}(e_j, (\text{PS}(I_i)), O_j) \equiv \forall_t \, , \text{w} \mid (t, PS(I_i)) \wedge$$

$$\dots..(P', S')) \wedge (p', \text{S}) \text{C } 8(\nexists p' \mid \text{C } (p', \text{S}) \wedge \text{C } (p, S) \wedge \text{Where PS(S)} \equiv s' \mid \forall p, \in (p, s')$$

به طور معمول ،نگرانی های حریم خصوصی با اثرات منفی مرتبط است یا به عنوان تاوانی درعواقب افشای اطلاعات که منجر به اجرای عملیات غیر مجاز است ،در نظر گرفته میشود.علاوه بر این به دلیل فرض دانش ناقص اشیا هوشمند ،این مدل برای ضبط خطر وقوع تاثیرات منفی ،توسعه یافته است.

4. چارچوب مدیریت حفاظت از حریم خصوصی

ما یک قالب مدیریت حفاظت از حریم خصوصی مبتنی بر تعامل سیستم های توزیعی تعاونی ارائه دادیم.1:محدود کردن عملیات غیر مجاز ،2:خنثی کردن عملیات های غیر مجاز.حفاظتی کامل است که با توجه به دانش ناقص اشیا هوشمند ،بتواند ازعملیاتی که در دسترس نیست جلوگیری کند یا آن را خنثی کند.در این مورد ،شبه مکنیزم های محافظت قابل اجرا هستند.به عنوان مثال برخی تکنیک های ناشناس را میتوان با درجه احتمال خاصی برای حفاظت از حریم خصوصی ارائه داد.تکنیک های ناشناس معمولا برای تحقیقات بالینی و پزشکی استفاده می شود[16] . با این حال، بسته به روش ناشناس، ما می توانیم حفاظت از حریم خصوصی با ارائه برخی از سطح های اعتماد اجرا کنیم.همچنین میتوان از مکانیزم مبتنی بر قانون برای استفاده از تعداد محدودی از عملیات های غیر مجاز ،استفاده کرد.در اینجا معیاری برای اندازه گیری درجه حفاظت حریم شخصی معرفی میکنیم.این معیار یک مدل پایه احتمالی که اثر یک مکانیزم برای محدود کردن یا خنثی کردن عملیات از تولید اطلاعات حساس ،به کار میرود.یک مکانیزم حفاظت اطلاعات راμ در نظر بگیرید که در فضای Sتعریف میشود برای جلوگیری از انجام عملیات های غیر مجاز:

$$\equiv \mathrm{PP}(e_j,\mathrm{S},\hat{O}_j^i(\mathrm{S}))\bar{\bar{\mu}}$$

برای مکانیزم مشابه آن ،استفاده ازین مکانیزم در فضای اطلاعات اشیای هوشمند ،ممکن است با توجه به معیار سطح حفاظت حریم شخصی ،عدم قطعیت را نشان دهد.ما میتوانیم این را به عنوان احتمال شرطی حفاظت اطلاعات داده شده توسط μ که فضایی مانند I_i میدهد ،مانند:

$$\mathrm{PPL}(e_j,I_i,\mu_t)=\mathrm{P}(\bar{\bar{\mu}}\,|\,I_i)$$

به عنوان مثال $a\epsilon$تابع خصوصی دیفرانسیل آن $(1-2\epsilon)$[17]در نظر گرفته میشود.مقدار مورد نظر بدست آمده از چندین بار آزمایش دیفرانسیل حریم شخصی این است :

$$E(z) = n(1 - 2\epsilon)$$

که این مربوط به سطح حفاظت از حریم شخصی با مقدار داده شده توسط $1-2\epsilon$.

مکانیزم حفاظت حریم شخصی ،در دو مدل کامل یا مشابه میتواند در دو سطح رخ دهد.مرحله اول : حفاظت در سطح عملیات که در آن میتوان عملیات غیر مجاز را شناسایی کرد.به عنوان مثالق قانون مبنی بر موتورهایی که

دارای مجوز هستند.در مرحله دوم ،دسترسی هایی بر اساس استفاده از حفاظت سطح اطلاعات برای خنثی سازی اجرای غیر مجاز عملیات.مثالی در مورد دسترسی دیفرانسیل حریم خصوصی ،تلاش برای تحریف اطلاعات توسط نویز انداختن است. مکانیزم حفاظت از حریم خصوصی را می توان در مدت عملیات O^{μ} و اطلاعات I^{μ} مدلسازی کرد: $\mu = <O^{\mu}, I^{\mu} >$

مکانیزم حفاظت از حریم خصوصی را میتوان به عنوان" پیشگیرانه "و" جریمه ای "دسته بندی کرد.اطلاعات پیشگیری بر اساس مکانیزم بوجود آوردن حفاظت در برابر با دستکاری اطلاعات در طول تعامل برای محدود کردن افشای اطلاعات حساس. نمونه هایی از این مکانیسم ها تکنیک های ناشناس هستند [4] ،یا متد رمز گزاری [18] اجرا شده روی حفاظت حریم شخصی.مکانیزم حفاظت پیشگیری کننده تلاش میکند برای محدود کردن عملیات از تولید اطلاعات حساس.به عنوان مثال ،ماشین های قانونمند دارای مجوز ،با توجه به قوانین مشخص ،از انجام عملیات غیر مجاز جلوگیری میکنند.دسترسی متنبهانه در مکانیزم حفاظت حریم شخصی در جایی است که پیشگیری اجرا نشده یا کافی نیست.مکانیزم جریمه ای در شرایطی بر اساس تعامل طرفین است.توافق دوطرفه ،ساختار نقش حفظ حریم شخصی را توصیف میکند.که این توافق شامل عملیات غیر مجاز و فرآیند های جریمه ای است.یک مثال مانند ، شرایط و ضوابط و مسئولیت های حقوقی مرتبط که بر روی اشیا هوشمند توافق شده است.اگر هرگونه عملیات غیر مجازی انجام شود عواقبی برای این اشیا هوشمند معیوب در نظر گرفته شده است.

4.1 تعامل بر اساس حفاظت از حریم خصوصی

تعامل مکانیزمی است که اشیا هوشمند اتخاذ شده اند برای هماهنگی با مسائل مربوط مانند توانایی ها ،علاقه ،دانش و منابع.اجازه دهید تعامل $<\delta, e_i , e_j, IP>$ این باشد در حالی کهδ نوعی از وابستگی متقابل است.اشیا هوشمند e_i و e_j در گیر این تعامل هستند.IP پروتکل تعاملی بدست آمده توسط اشیا هوشمند است. IPیک پروتکل بر اساس پیام است که توسط $<M , S_m>$ مشخص شده است. M مجموعه پیام است وS_m توالی پیام هاست.M(IP) اشاره

دارد به مجموعه IP وS_m (IP) اشاره دارد به آدرس توالی های همراه IP.در این کار ما تمرکزمان روی گسترش پروتکل تعامل با توانایی حفظ حریم خصوصی است.

در این زمینه IP میتواند به عنوان مجموعه ای از عملیات ها که اطلاعات را جمع آوری و انتشار میدهد ،مدل سازی شود که توسط $< O^{IP,1}, \ldots, O^{IP,q}, \ldots, O^{IP,Q} >$=IP مشخص میشود.

همچنین مکانیزم حفاظت اطلاعات یک دنباله از عملیات هاست : $O^{\mu} < O^{m,1}, \ldots, O^{m,d}, \ldots, O^{m,D} >$

$1 \le d \le D$ ،.

چارچوب پیشنهادی برای حفظ حریم شخصی پروتکل تعاملی را با عملیات مکانیزم حفظ حریم شخصی گسترش میدهد.ما سه مدل گسترش را پیشنهاد میدهیم. در مرحله اول، عملیات مکانیسم حفاظت به عنوان پیشوند به عملیات پروتکل تعامل الحاق میشود.به عنوان مثال ،قبل از اینکه اطلاعات پزشکی توسط سنسورهایی که با اشیاء هوشمند در یک آزمایشگاه ارتباط دارند ، جمع آوری شود ،عملیات مورد نظر رمز گزاری میشود.نتیجه به عملیاتی که در پروتکل تعامل است و میتواند اطلاعات رمزگزاری شده را به اشیا هوشمند در آزمایشگاه ارائه دهد ،ارسال میشود.

$< O^{m,1}, \ldots, O^{m,d}, \ldots, O^{m,D} >$

حفاظت از حریم خصوصی را برای این تعامل به طور معمول می تواند به عنوان مکانیسم مجازات خطاب شود.به عنوان مثال ،گزارش به ناظر جزییات و نظم و انضباط را میتوان در پروتکل تعاملی ثبت کرد.سوما توسعه بر اساس ادغام عملیات مکانیسم حفاظت از حریم خصوصی با پروتکل تعامل بر اساس این است که عملیات از کندی پروتکل تاثیر نمیگیرد.دنباله ای از عملیات های مکانیزم در پروتکل ،توسط اطلاعات موجود تعیین شده است.برای مثال ،تهیه کنندگان IaaS برای برای پیوستن مصرف کنندگان به سوم شخص برای تجزیه تحلیل "مصرف کنندگان ناشناس" اطلاعات ونظرات کلی در مورد الگوی مصرف را دریافت میکنند.

$< O^{IP,1}, \ldots, O^{m,1}, \ldots, O^{IP,Q}, \ldots O^{m,d}, \ldots, O^{IP,\acute{q}}, \ldots O^{m,\acute{d}}, \ldots O_K^{IP} >$

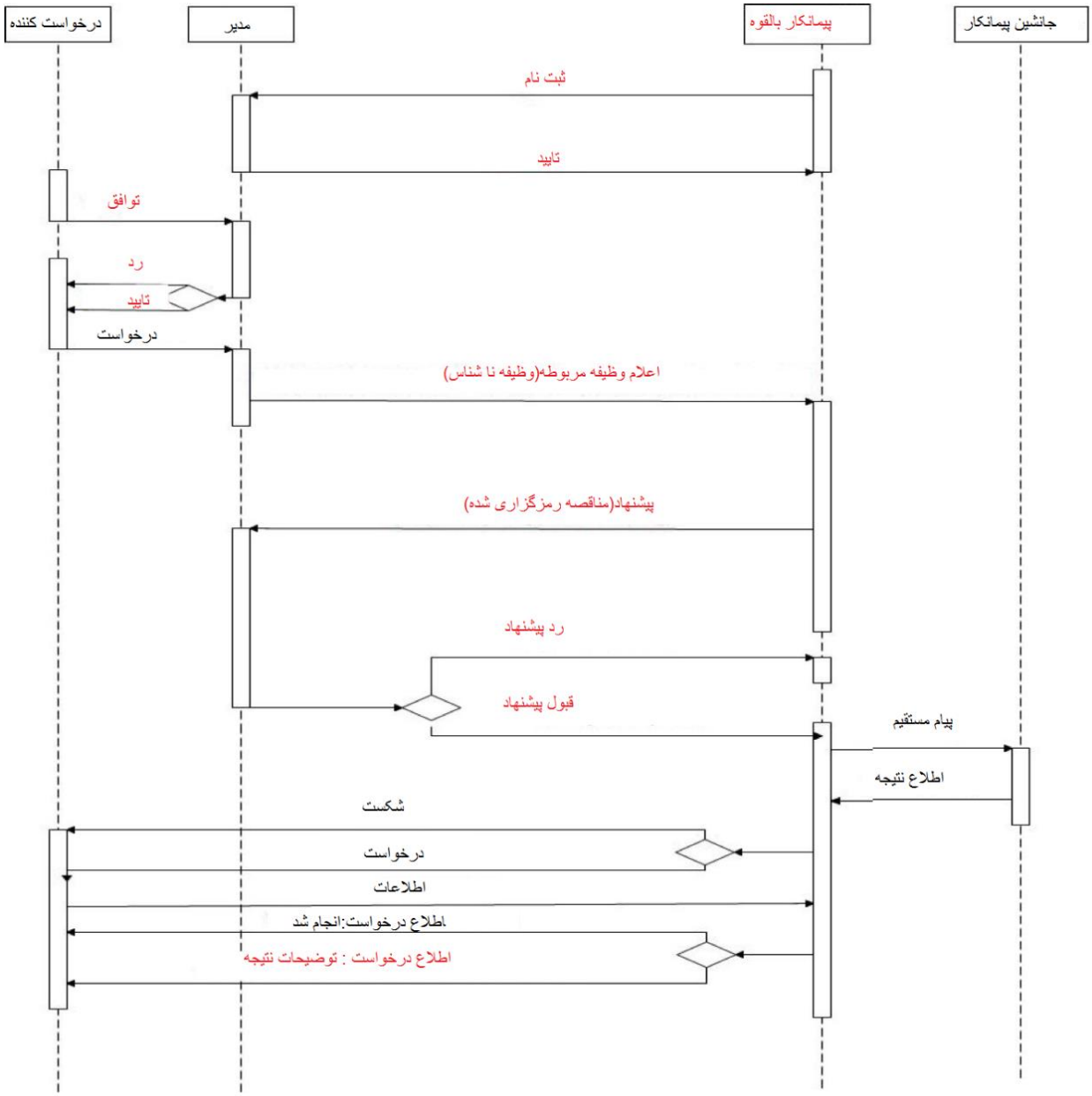
عملیات در مکانیزم حفاظت از حریم خصوصی ممکن است به نوع جدیدی از پیام ها که برای پیام های مجموعه ای ازپروتکل ،علاوه بر گسترش دنباله ای از پروتکل تعامل ،نیاز داشته باشد.از طریق انطباق مکانیزم حریم خصوصی در سطح پروتکل های تعامل ،محدود میشود به اشیا هوشمندی که حریم خصوصی را میتوانند با یک سطح حفاظت

شده حریم شخصی قابل قبول در تعاملشان حفاظت کنند. دنباله ای ازعملیات در پروتکل تعامل در حریم خصوصی مبتنی بر پروتکل تعامل تغییر نکرده است اما عملیات مکانیسم حفاظت از حریم خصوصی اعمال می شود.این می تواند از اجرای عملیات های غیر مجاز و تبدیل اطلاعات حساس ضمنی به صریح ،جلوگیری کند و یا آنرا خنثی کند.هر یک از مکانیزم های اعمال شده ،دارای ارزش سطح حفاظت حریم شخصی است.مکانیزم های مختف را میتوان با یک پروتکل تعامل به شکل یک حریم خصوصی مبتنی بر پروتکل تعامل ،یکپارچه کرد(PB_IP). با قرار دادن یک فرض در استقلال مکانیسم های محافظت ،سطح حفاظت حریم شخصی در تمام مکانیزم های اعمال شده افزایش پیدا کرده است.

$$PPL(PL\_IP) = \coprod_{j| \in (\mu, PB\_IP), \in (ej, W)\forall \mu,} PPL(ej, M(PB\_IP), \mu))$$

چارچوب مدیریت حفاظت از حریم خصوصی ،اشیا هوشمند را به شناسایی اطلاعات حساس با گرفتن اطلاعات و در معرض قرار گرفتن مرز خود ،قادرمیکند. به این ترتیب که قادر به شناسایی اطلاعات حساس و گسترش پروتکل تعامل با مکانیسم های حفاظت از حریم خصوصی کافی بدون تاثیر از کندی پروتکل و حمایت از معماری ، خواهد بود. قرارداد خالص پروتکل (CNP) یک پروتکل تعامل است که در ابتدا برای حل مشکل توزیع در یک طبقه خاص از سیستم های توزیعی تعاونی ،پیشنهاد شده است. این پروتکل می تواند برای حل وابستگی متقابل مبتنی بر توانایی کار کند.این پروتکل میتواند چند نقش را برای شناسایی اجزا شناسایی کند ،مانند مدیری که وظیفه و پیمانکاران توانمند را که قادر به اجرای این کار هستند را اعلام میکند.پیمانکاران توانمند میتوانند این کار را به بهترین نحو انجام دهند و پس اجرای آن جایزه بگیرند [19]. CNP را می توان برای اعمال اشیا هوشمند در اینترنت اشیا و اتخاذ یک معماری مبادله که در آن کارگزاران بر اساس قانون مبادله نماینده میشوند ،اعمال کرد و درخواست کنندگان درخواست خود را به کارگزاران محول نمایند.یک پروژه فضایی هوشمند بر اساس محیط اینترنت اشیا در آزمایشگاه تحقیقاتی CDS-ENG اجرا شده است.که این شامل حسگرها، تجهیزات، خدمات و منابع داده که دربرنامه های کاربردی است ،میشود. در داخل این محیط، اشیاء هوشمندی هستند که سطح اشیا را میسازند. خدمات در این

محیط ،استفاده از منابع موجود در فضا و ارائه راه حل برای برنامه های کاربردی است.سطح مبادبه ویژگی هایی را آماده میکند برای به ادغام با منابع از محیط زیست از جمله داده ،حوادث و ابهامات.



شکل 1 .حفظ حریم خصوصی

برای حل وابستگی متقابل قابلیت در این تنظیم، اشیاء هوشمند CNPبه عنوان پروتکل تعاملی که درآن لایه مبادله به عنوان یکی از اجزاعمل می کند به تصویب رسید.ارائه مبتنی بر بهره برداری از CNP می تواند به این صورت مدلسازی شود:

CNP ={ <درخواست(اعلام وظیفه)،اعلام_وظیفه()،پیشنهاد (درخواست)، قبول_برپانگه داشتن، آگاه کردن، واکنش ، اعلام_وظیفه (وظیفه)، پاسخ>و < اعلام_وظیفه(وظیفه)، پیشنهاد(درخواست)،امتناع_درخواست>و< اعلام_وظیفه(وظیفه)، امتناع> }

اشیا هوشمند اطلاعاتی که از انواع پیام و دنباله پیام ها در CNP استفاده میکنند را به اشتراک میگذارد.به هر حال ،نگرانی حفظ حریم خصوصی در به اشتراک گذاری اطلاعات در CNP در نظر گرفته نشده و این پروتکل فاقد حفاظت از حریم خصوصی است.در این پروتکل : $I_{r,t}$={انجمن درخواست کنندگان کار} و مرز در معرش قرار گرفتن : $I_{r,t}$ همان $E_{r,t}$={مدیر} است.اتصال اطلاعات} = $I_{r,t}$ و مرز در معرض قرار گرفتن $I_{r,t}$ برابر $E_{r,t}$= ∅ است.

{نتیجه اطلاع از عملیات} = $I_{r,t}$ و مرز در معرض قرار گرفتن $I_{r,t}$ برابر {شخصیت } = $E_{r,t}$

زمانی که اشیا هوشمند به دنبال تشخیص دیگر اشیا یی که قادر انجام وظیفه خود هستند شروع به اعلام وظیفه در فاز CNPمیکنند. اعلام وظیفه شامل هویت درخواست کننده و مشخصات کار است.اعلام وظیفه با تمام اشیای هوشمند با هدف پیدا کردن پیمانکاران بالقوه رقابت برای این کار ،به اشتراک گذاشته میشود. مرز قرار گرفتن در معرض ترکیبی از کار و هویت تنها شامل مدیر میشود. از این رو این اطلاعات حساس می شود. در زمینه مدیریت اطلاعات CNP،در این حالت است که به شرح زیر است:

CNP= {درخواست (اعلام وظیفه);اعلام وظیفه }

به عنوان نتیجه ،چارچوب مکانیزم حفاظت در سطح اطلاعات مناسب برای کار است و داده پراکنی شناسایی پیمانکاران بالقوه.

نمونه ای از چنین مکانیزمی تکنیک های ناشناس است. همچنین به منظور کاهش پیمانکاران بالقوه به طوری که اشیا هوشمند قابلیت مربوط به وظیفه آنها را دارند ، ما مراحل ثبت نام در آغاز پروتکل را معرفی کردیم. از آنجا که اطلاعات باید با مدیر به اشتراک گذاشته شود و آنها ممکن است به عنوان اطلاعات کمکی در کنارمدیر خدمت

کنند،استفتده از مکانیزم پیشگیرانه ممکن نیست.این یکپارچه سازی مکانیزم مجازات را پیشنهاد میدهد. برای حالت اعلام کار حفظ حریم خصوصی بر اساس CNPبه عنوان زیر است :

CNP= { (اعلام وظیفه_مربوط(کار بی نام);درخواست(اعلام وظیفه)}

در بخش دیگری از CNP، اطلاعات مناقصه در رابطه با هویت پیمانکاران بالقوه به شرکت برنده در نهاد کارگزار ارسال خواهد شد. ترکیبی از ارزش مناقصه وتشخیص هویت داوطلب در رابطه حساس با مدیر است[20] به خاطر در معرض قرار گرفتن این اطلاعات که $E_{c,b}$ = Ø است.با این حال CNP این اطلاعات را به اشتراک میگذارد :

CNP= { هدف ،پذیرش پیشنهاد}

یکی از مکانیسم محافظت از حریم خصوصی در این زمینه استفاده از مکانیسم های پیشگیرانه در سطح اطلاعات با استفاده از مکانیزم پیشنهادی [21] می باشد که در آن محاسبات روی اطلاعات رمزگذاری شده و کارگزار از ارزش مناقصه آن مطلع نیست. با استفاده از این مکانیزم پروتکل با فرایندهای اضافی به رمز در آوردن اطلاعات مناقصه گسترش میابد.

PB_CNP= { پذیرش پیشنهاد، به رمز در آوردن اطلاعات مناقصه}

$E_{r,j}$ تنها شامل پیمانکاری که پاسخ اطلاعات حساس در رابطه با مدیر را کوتاه میکند. با این حال، CNP سنتی این اطلاعات را با مدیر به اشتراک میگزارد. برای محافظت از این اطلاعات، نیازبه جلوگیری از عملیات به اشتراک گذاری (مکانیسم پیشگیرانه در سطح عملیاتی)دارد.که این باعث میشود پیمانکار صاحب کار را شناسایی کرده و اطلاعات را به صورت مسقیم با انها به اشتراک بگذارد.همچنین ممکن است با استفاده از روش های رمزنگاری ،اطلاعات نتیجه را با کلید عمومی درخواست به رمز در بیاورد(مکانیسم پیشگیری در سطح اطلاعات). در هر مورد، پیمانکار باید صاحب درخواست را شناسایی کند.{آگاه سازی}= CNP و{تحقق صاحب ،درخواست کننده آگاه سازی} = PB_CNP.انجام دادن عملیات پیشنهادی پروتکل را از نظر پیام و انجام مکانیزم حفاظت مانند زیر گسترش میدهد. حفظ حریم خصوصی بر اساس CNPنیز درعکس. 1. به تصویر کشیده شده است.

PB_CNP={

<توافق، تایید ،درخواست (اعلام وظیفه) ،اعلام وظیفه (وظیفه ناشناس) ،پیشنهاد (مناقصه رمزگذاری شده)، پیشنهاد_قبول شده ،اطلاع درخواست>، <اعلام وظیفه(وظیفه ناشناس) ، پیشنهاد (مناقصه رمزگذاری شده)، پیشنهاد_رد شده > ،< اعلام وظیفه (وظیفه ناشناس) ، رد شدن> ، <ثبت نام ، پذیرش >}

برای توضیح استفاده از حریم خصوصی بر اساس CNP ،نرم افزار تشخیص حرکت یک مانند e_m یک شی هوشمند است که با استفاده از سنسور تشخیص حرکت در فضای هوشمند اما نیاز به قابلیت های دیگر اشیاء هوشمند مجهز با سنسور نور دارد ، تشخیص چهره، تشخیص لرزش و اندازه گیری درجه حرارت. بر اساس ساختار CNP ،" تشخیص حرکت "اعلام وظیفه میکند به کارگزار خدمات برای شناسایی اشیاء هوشمند که قادر به اجرای وظیفه هستند.در زمینه فضای هوشمند W ، e_m یک پیام برای حسگر نور($I_{m,l}$) و حسگر شناسایی چهره $I_{m,f}$او تشخیص لرزش$I_{m,v}$ و تشخیص دما $I_{m,t}$ ایجاد میکند که خدمات و ایمنی را به اشخاص داخل موزه ارائه میدهد.عملیات O^{rec} یک عملیاتی است که می تواند اقدامات بعد از نهادهای بر اساس منافع خود را با درجه ای از عدم قطعیت پیش بینی کند.

اجرای $^{rec}(\{I_{m,I}, I_{m,f}, I_{m,v}, I_{m,g}\}, I^{aux}) = I_{m,s}\bar{\bar{o}}$

با این حال، با استفاده از PB_CNP، وظایف نا مشخص واطلاعات حساس محافظت شده است.

5. نتیجه گیری

اینترنت از چیزهایی که شامل تعداد زیادی از برنامه های کاربردی است که در حال حاضر بخشی از زندگی مردم است.اشیا شامل آنهایی است که به عنوان اشیای هوشمند مدل سازی شده و می تواند یکپارچه با یکدیگر در یک پلت فرم مبتنی براتصال به اینترنت باهم ارتباط برقرار کنند." اشیا "در اینترنت اشیا به طور فعال در محیط زیست برای ارائه خدمات برنامه های کاربردی شرکت میکنند. با این حال، به دلیل افزایش درگیری های مردم و یا دستگاه هایشان در این برنامه ها ، نگرانی های حریم خصوصی تبدیل به یک چالش عمده شده است. در این کار، یک مدل CDSاز آن پیشنهاد شده است.در تنظیمات این اشیای هوشمند اطلاعات حساسی وجود دارد و آنها تمایلی به

اشتراک گذاشتن آن ندارند. حساسیت اطلاعات در معرض مرز حاوی اشیای که اطلاعات میتواند در آن به اشتراک گذاشته شود ،تعریف شده است. پیشگیری یا خنثی کردن عملیات های غیر مجاز از انجام عملیات روی اطلاعات نگرانی اصلی حفاظت از حریم خصوصی است.ا ین کارPPLرا به عنوان یک اقدام برای رسیدگی به سطح عدم قطعیت در مکانیسم حفاظت از حریم خصوص پیش نهاد میدهد. در نتیجه، این کاریک چارچوب مدیریت حفاظت از حریم خصوصی است که در برنامه های کاربردی اینترنت اشیا بر اساس -CDSاجتماعی پیشنهاد میشود. که آن ازپروتکل تعامل و عملیات حفاظت برای تولید یک پروتکل تعامل حریم خصوصی استفاده میکند. برنامه چارچوب مدیریت حفاظت از حریم خصوصی در قرارداد پروتکل شبکه است که در این کار ارائه شده است.

References

1. Atzori L, Iera A, Morabito G. From smart objects to social objects: The next evolutionary step of the internet of things. IEEE Communications
Magazine 2014;52(1):97-105.
2. Adaptive security and privacy management for the internet of things (ASPI 2013). Proceedings of the 2013 ACM conference on pervasive and
ubiquitous computing adjunct publicationNew York, NY, USA: ACM; 2013. .
3. Negotiation-based privacy preservation scheme in internet of things platform. Proceedings of the first international conference on security of
internet of thingsNew York, NY, USA: ACM; 2012. .
4. Differential privacy: A survey of results. Proceedings of the 5th international conference on theory and applications of models of
computationBerlin, Heidelberg: Springer-Verlag; 2008. .
5. A utility-theoretic approach to privacy and personalization. Proceedings of the 23rd national conference on artificial intelligence - volume
2AAAI Press; 2008. .
6. Such JM, Espinosa A, García-Fornes A. A survey of privacy in multi-agent systems. Knowl Eng Rev 2012.
7. Toubiana V, Nissenbaum H, Narayanan A, Barocas S, Boneh D. Adnostic: Privacy preserving targeted advertising _. 2010.
8. Ghenniwa HH. Coordination in cooperative distributed systems. ; 1996.
9. Bo Lang , Ian Foster , Frank Siebenlist , Rachana Ananthakrishnan , Tim Freeman. A multipolicy authorization framework for grid security.
Proceedings of the Fifth IEEE Symposium on Network Computing and Application 2006.
10. Paul M. Schwartz, Daniel J. Solove. The PII problem: Privacy and a new concept of personally identifiable information. 2011.
11. Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam M. L-diversity: Privacy beyond k-anonymity. ACM Trans.Knowl.Discov.Data
2007 mar;1(1).
12. On the tradeoff between privacy and utility in data publishing. KDD} '09: Proceedings of the 15th {ACM} {SIGKDD} international
conference on knowledge discovery and data miningNew York, {NY {USA}: ACM}; 2009. 0036.
13. Facebook’s facial recognition software is now as accurate as the human brain, but what now? [Internet].

14. Facebook Creates Software That Matches Faces Almost as Well as You Do [Internet].
15. Samani A, Ghenniwa HH. Privacy in IoT: A model and protection framework. London Ontario: ; August 2014. Report nr CDS-EnG-report-
Privacy in IoT: A Model and Protection Framework-TR -0827 2014.
16. Sweeney L. K-anonymity: A model for protecting privacy. Int.J.Uncertain.Fuzziness Knowl.-Based Syst. 2002 oct;10(5):557-70.
17. Mechanism design via differential privacy. Proceedings of the 48th annual IEEE symposium on foundations of computer scienceWashington,
DC, USA: IEEE Computer Society; 2007. .
18. Targeted advertising ... and privacy too. Proceedings of the 2001 conference on topics in cryptology: The cryptographer's track at
RSALondon, UK, UK: Springer-Verlag; 2001. .
19. Smith RG. Computers, IEEE Transactions on Title={the Contract Net Protocol: High-Level Communication and Control in a Distributed
Problem Solver 1980 dec.;C-29(12):1104.
20. Privacy preserving auctions and mechanism design. Proceedings of the 1st ACM conference on electronic commerceNew York, NY, USA:
ACM; 1999.
21. Secure combinatorial auctions by dynamic programming with polynomial secret sharing. In proceedings of the sixth international financial
cryptography conference Springer; 2002.