V2C: um veículo seguro para a estrutura em nuvem para provisionamento de serviços sob demanda e virtualizado

Article · August 2012
DOI: 10.1145/2345396.2345422

5 authors, including:

Anand Kannan
KTH Royal Institute of Technology
14 PUBLICATIONS **75** CITATIONS
SEE PROFILE

Ayush Sharma Lasell
College
7 PUBLICATIONS **74** CITATIONS
SEE PROFILE

V2C: um veículo seguro para a estrutura em nuvem para provisionamento de serviços sob demanda e virtualizado

Sathyanarayanan Rangarajan
Fraunhofer AISEC
Parkring 4, 85748 Garching, Germany
sathya.rangarajan@aisec.fraunhofer.de

Monica Verma
Siemens CERT
Otto-Hahn-Ring 6, 81739 Munich, Germany
monica.verma@siemens.com

Anand Kannan
School of Information and Communication Technology
KTH, Royal Institute of Technology, Stockholm, Sweden
anandk@kth.se

Ayush Sharma
Fraunhofer AISEC
Parkring 4, 85748 Garching, Germany
ayush.sharma@aisec.fraunhofer.de

Ingmar Schön
Fraunhofer AISEC
Parkring 4, 85748 Garching, Germany
ingmar.schoen@aisec.fraunhofer.de

RESUMO

A computação em nuvem revolucionou o setor de TI ao habilitar um modelo de provisionamento de recursos virtualizado para organizações. O modelo de provisionamento NaaS (Network-as-a-Service) permite novas maneiras de fornecer recursos de rede virtualmente isolados e sob demanda em modelos de provisionamento de nuvem existentes, resultando em melhor desempenho de esforço, throughput de dados escalável, latência reduzida, e reduzida complexidade de configuração. Neste artigo, propomos a V2C, uma infraestrutura eletro-veículo-nuvem que integra o NaaS ao ecossistema automotivo e permite o fornecimento de serviços baseados em veículos para usuários de automóveis. No entanto, a V2C apresenta vários desafios de segurança e o principal objetivo deste artigo é propor um modelo de provisionamento seguro para resolvê-los.

Categorias e Assuntos Descritores

C.2.1 [Arquitetura e Projeto de Rede]: Comunicações de rede; C.2.4 [Sistemas Distribuídos]: Cliente / servidor;

D.4.6 [Segurança e Proteção]: Controle do fluxo de informações; D.4.8 [Performance]: Medidas

Termos Gerais

Design, gerenciamento, desempenho e segurança

Palavras-chave

Redes veiculares, arquitetura de segurança, rede em nuvem, redes de próxima geração

1. INTRODUÇÃO

A computação em nuvem é, sem dúvida, uma das principais mudanças de jogo experimentadas pela indústria de TI durante a última década. Definido pelo Instituto Nacional de Padronização e Tecnologia (NIST) em [1] e [2], a computação em nuvem permitiu gradativamente a transição da infraestrutura corporativa para a nuvem, sendo a força motriz dessa transição um gasto de capital reduzido (CAPEX) associado a um gasto operacional reduzido (OPEX).

A computação em nuvem até agora foi direcionada apenas para empresas de grande e médio porte. No entanto, com o advento da penetração generalizada de serviços em nuvem em telefones celulares e outros dispositivos, as nuvens ultrapassaram a infraestrutura simples e entraram em nossas vidas diárias. Além da quantidade de tempo gasto em casa e no trabalho, gasta-se muito tempo viajando de carro. O desempenho e a qualidade dos recursos atuais oferecidos em um carro, como serviços de navegação, serviços de infoentretenimento, etc., dependem muito do hardware e software disponíveis no carro. Esses recursos podem ser aprimorados ainda mais pela integração de serviços em nuvem em automóveis. Isso não apenas oferece maior e melhor capacidade de processamento e armazenamento, mas também facilita a redução da quantidade de hardware e software existentes no carro e abre caminho para uma nova gama de serviços.

No entanto, a computação em nuvem, semelhante a outras tecnologias em crescimento, tem seu próprio conjunto de problemas. A disponibilização qualitativa de serviços de navegação e infoentretenimento para veículos móveis não requer apenas recursos de computação e armazenamento sob demanda, mas também depende muito da largura de banda de rede disponível. Os modelos existentes de provisionamento de serviços viz. Software como serviço (SaaS), Plataforma como serviço (PaaS) e Infraestrutura como serviço (IaaS), exibem desempenho inseguro, baixa confiabilidade e taxa de transferência devido à falta de recursos de rede concretos e maduros [3].

O projeto europeu SAIL [3] introduziu o Network-as-a-Service (NaaS), que integra fortemente o provisionamento de recursos de rede virtualizados, juntamente com os modelos existentes de provisionamento de serviços, viz. SaaS, Paas e IaaS. Além disso, o SAIL introduz a arquitetura CloNe [4], que aplica uma arquitetura genérica de Cloud Network (CloNe) e permite que os usuários do serviço solicitem parâmetros de rede, junto com as restrições de serviço desejadas. Portanto, o NaaS visa negar a falta de confiabilidade em modelos existentes de provisionamento de serviços em nuvem e promover

confiabilidade e garantia de QoS [3]. Assim, é seguro afirmar que os diversos requisitos do modelo de provisionamento de serviços em nuvem para carros serão atendidos por um modelo de provisionamento de serviços semelhante ao proposto pela arquitetura CloNe.

Este documento amplia ainda mais a arquitetura de cloNe e a arquitetura de segurança CloNe existentes, e as modifica para o ecossistema de automóveis. A principal contribuição do papel é a definição de um modelo de provisionamento de serviços em nuvem, ou seja, a infraestrutura V2C, personalizada para o ecossistema automotivo, e uma arquitetura de segurança que se integra ao modelo de provisionamento V2C e assegura a infraestrutura completa de fornecimento. Além disso, casos de uso e exemplos de cenários são descritos para provisionamento de serviços em nuvem em automóveis.

O artigo está organizado da seguinte forma. A Seção 2 fornece o trabalho relacionado com as arquiteturas de segurança em nuvem, provisionamento de serviços em nuvem em carros e outras áreas de pesquisa relacionadas.Secção 3Descreve a arquitetura customizada do CloNe, ou seja, infraestrutura V2C, para ser usada no automo - ecossistema bile. A seção 4 é desenvolvida sobre a arquitetura de segurança, que protege a arquitetura de provisionamento de serviços descrita na Seção 3. A seção 5explica exemplos de casos de uso para o modelo de provisionamento de serviços para carros, como navegação baseada em nuvem e infotainment baseado em nuvem.Seção 6 resume o resultados do artigo, e compara-o com o estado da arte. A secção 7 conclui o trabalho e mostra futuras direcções de trabalho.

2. TRABALHO RELACIONADO

A comunicação veicular experimentou uma rápida mudança de foco de um tópico orientado para a pesquisa para a integração em carros prontos para produção dos principais fabricantes da indústria, ou seja, o carro com WiMAX da Intel [5] e o carro LTE da Toyota. 6]. Desde a alocação do espectro para a Inter-Vehicle Communications (IVC) pela Federal Communications Commission e a emenda do padrão IEEE 802.11p para Acesso Sem Fio em Ambientes Veiculares (WAVE) [7], vários trabalhos de pesquisa foram realizados sobre comunicação veículo-veículo e veículo-infra-estrutura [8,9]. Daiheng Ni [10] propôs uma arquitetura que permite aos veículos se comunicarem com qualquer infra-estrutura rodoviária disponível, a fim de transmitir a velocidade e a localização do veículo para um servidor localizado centralmente. Jegor Mosyagin [6] propôs o uso da tecnologia 4G para comunicação veicular e os experimentos cobertos no jornal exibiram taxas máximas de transferência de dados de 10 Mbps para um veículo viajando a uma velocidade máxima de 140 km / h. No entanto, tecnologias mais recentes, como LTE e 4G, apresentam novos desafios de segurança.

Seddigh et al. [11] apresenta um estudo dos avanços e desafios de segurança associados a tecnologias sem fio 4G emergentes. O documento descreve áreas potenciais para futuras vulnerabilidades e avalia áreas de segurança 4G que merecem atenção imediata. Além disso, o documento propõe um trabalho futuro potencial para mitigar esses desafios. Yu-Hunag Chu

[12] propuseram e implementaram um novo design de arquitetura de rede adequado para modelos em nuvem. Este modelo é experimentalmente comprovado como sendo rentável a partir de uma perspectiva de especialmente para um cenário em que os recursos de rede são provisionados sob demanda. O fornecimento seguro e sob demanda de recursos de rede utilizando as novas tecnologias de rede, como a LTE, é a base de nosso estudo. Este artigo apresenta nossa visão sobre a evolução de auto-celulares mais inteligentes que estão conectados à nuvem usando tecnologias avançadas (de rede) de maneira segura.

3. O MODELO V2C

A arquitetura original do CloNe [4] define um modelo de provisionamento de recursos de rede virtualizado, que permite uma forte integração entre os modelos existentes de provisionamento de serviços virtualizados, viz. SaaS, Paas e IaaS e o modelo proposto de provisionamento NaaS. Além disso, o modelo de provisionamento no CloNe foi definido em vários níveis de hierarquia de serviços e transcende vários limites administrativos. O modelo V2C proposto neste documento compartilha as mesmas propriedades básicas do ecossistema CloNe, ou seja, vários níveis na hierarquia de serviços, vários limites administrativos e provisionamento de recursos de rede sob demanda. Esta seção descreve como a arquitetura CloNe é usada como um modelo de referência e mais personalizada de acordo com as especificações do ecossistema automotivo. Seções ?? e3.3descrever detalhadamente o ecossistema automotivo e a infra-estrutura de provisionamento V2C.

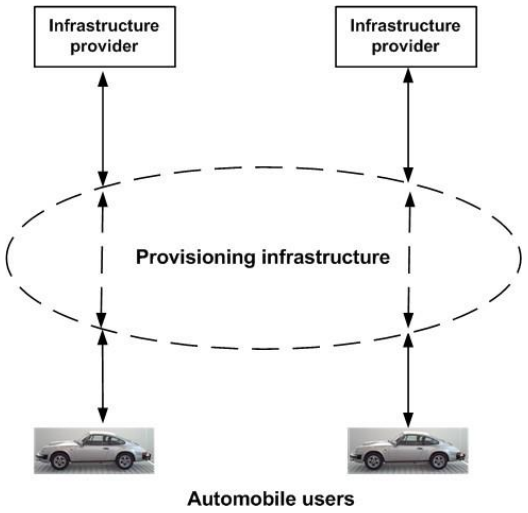

Figure 1: Abstract architecture of cloud service provisioning model

Arquitetura Abstrata

A Figura 1 mostra uma arquitetura abstrata do modelo V2C proposto para automóveis. Os dois papéis centrais na arquitetura abstrata são o usuário de automóvel e o provedor de infra-estrutura. O usuário do automóvel inicia uma solicitação de serviço ao provedor de infra-estrutura utilizando a infraestrutura de provisionamento, que cuida da propagação da solicitação de serviço abstrato para o provedor de infra-estrutura e pode traduzir a solicitação em expressões mais concretas. A solicitação é recebida pelo provedor de infra-estrutura, que é responsável pela delegação da solicitação de serviço em diferentes unidades administrativas (internas ou externas) e gerencia a colaboração entre essas solicitações.

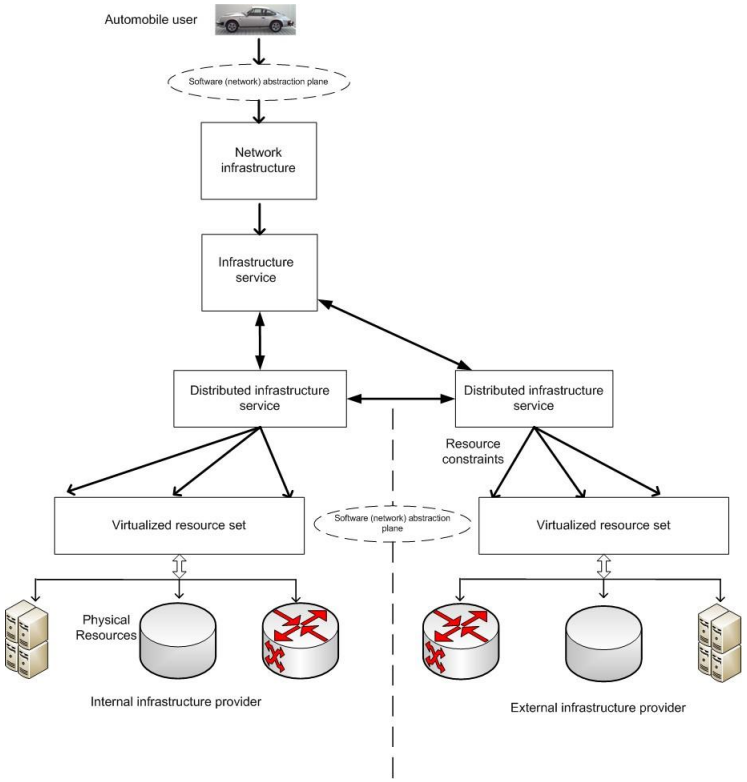

Figure 2: Distributed architecture of cloud service provisioning model

unidades através de SLAs internos e externos. O provedor de infra-estrutura é responsável por garantir que as restrições gerais de QoS do usuário de automóvel sejam atendidas. Portanto, ele precisa ter um controle rígido sobre todo o caminho de propagação, incluindo a infraestrutura de provisionamento.

A infra-estrutura de provisionamento é visível apenas para o usuário de dispositivos móveis na forma de uma interface (possivelmente integrada ao painel do carro) e, portanto, toda a infraestrutura de backbone será opaca para o usuário. Isto é extremamente importante para assegurar uma penetração de serviços suficiente em uma base diversificada de usuários finais. O usuário de automóvel deve ser agnóstico quanto aos detalhes exatos de hardware e software da infra-estrutura de backbone, e deve ser permitido fornecer sua solicitação de serviço desejada usando termos e expressões abstratas. O pedido do usuário do automóvel será encapsulado dentro dos pacotes VXDL [13], que é o mesmo formato usado pelo CloNe.

Arquitetura detalhada

A Figura 2 descreve uma versão mais detalhada da Figura 1 e inclui toda a distribuição por componentes do modelo de provisionamento do V2C. O provedor de infra-estrutura de função original é dividido em outros sub-papéis, a saber, provedor interno de infraestrutura e provedor externo de infraestrutura. Cada provedor de infra-estrutura virtualiza e provisiona seu próprio conjunto de recursos para o usuário final ou arrendatário. Um provedor interno de infra-estrutura é definido como a entidade que gerencia o conjunto de recursos armazenados no domínio administrativo do provedor de infraestrutura original. A segunda sub-função é o provedor externo de infra-estrutura, que controla seu próprio conjunto de recursos e está alojado fora dos limites administrativos.

serviços do provedor de infra-estrutura interna. O provedor de infraestrutura externo pode colaborar com o provedor de infraestrutura interna, se este não puder provisionar os recursos solicitados sozinho.

Cada provedor de infra-estrutura fornece uma interface de administração de recursos. A interface de administração de recursos oferece um conjunto de APIs e funções de gerenciamento para a entidade superior na hierarquia de nível de serviço. O conjunto de funções de gerenciamento inclui uma função de conversão de metas, uma função de gerenciamento de recursos e uma função de gerenciamento de falhas, empregada pelo provedor de infra-estrutura. A função de tradução de objetivos aceita solicitações abstratas de serviço do usuário automotivo e as traduz em especificações concretas de recursos usando um processo de tradução multinível. As especificações de recursos concretas são fornecidas ainda para a função de gerenciamento de recursos. Antes de implementar as especificações concretas no conjunto de recursos físicos subjacentes, a função de gerenciamento de recursos colabora com a função de gerenciamento de falhas e gera relatórios de falhas. Os relatórios de falhas gerados contêm informações relativas a recursos parcialmente ou completamente comprometidos ou que estão sofrendo flutuações de desempenho. As informações fornecidas pelos relatórios de falhas ajudam a função de gerenciamento de recursos a evitar a alocação incorreta de recursos para atender às solicitações do usuário automático.

Provisionamento de serviços

O automobilista envia uma solicitação de serviço ao serviço de infra-estrutura, que é um papel desempenhado pelo fabricante do automóvel, ou qualquer outro prestador de serviço escolhido pelo usuário do automóvel para fornecer o serviço solicitado.

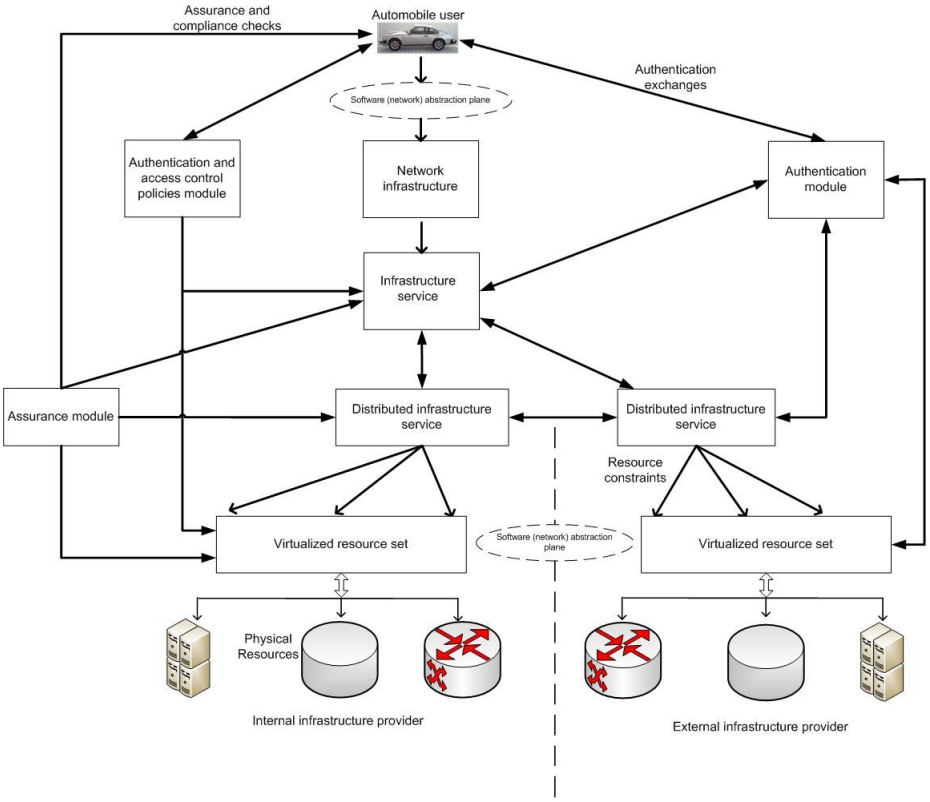

Figure 3: Security architecture of cloud provisioning model for automobiles

O serviço de infraestrutura emprega uma unidade de controle em seu centro, que é responsável por realizar a tradução inicial da solicitação do usuário. A solicitação abstrata inicial descreve as restrições SLO e QoS esperadas pelo usuário do automóvel. O serviço de infraestrutura também é responsável por armazenar um registro de componentes de serviços de infraestrutura distribuída, que são definidos como subconjuntos do componente de serviço de infraestrutura. Cada domínio administrativo abriga um componente de serviço de infraestrutura distribuída que é responsável por aceitar a solicitação de serviço do componente de serviço de infraestrutura. O serviço de infraestrutura distribuída traduz ainda mais a solicitação em configurações de recursos concretas e as fornece ao provedor de infraestrutura utilizando a interface de administração de recursos.

O componente de serviço de infraestrutura visa provisionar a solicitação de serviço utilizando apenas os recursos presentes em seu respectivo domínio administrativo. No entanto, em alguns casos excepcionais, os recursos em seu domínio estão com excesso de pedidos, apresentam falhas técnicas, são comprometidos ou os recursos não são aceitáveis pelo usuário no ponto de preço em que são provisionados. Nesse cenário, o serviço de infra-estrutura provisiona os recursos disponíveis / aceitáveis de seu respectivo domínio administrativo e anuncia os requisitos de recursos remanescentes (incluindo os requisitos de segurança, não funcionais e econômicos) entre os diferentes serviços de infraestrutura distribuída concorrentes componentes. Os componentes do serviço de infraestrutura distribuída que podem provisionar os recursos com êxito respondem com suas respectivas referências remotas. O componente de serviço de infra-estrutura seleciona então o (s) componente (s) de serviços de infra-estrutura distribuída que provisionaria recursos principais. O componente de serviço de infraestrutura transmite as informações de endereço dos componentes de serviço de infraestrutura distribuída selecionados para o componente primário de serviço de infraestrutura distribuída e o segundo executa a resolução de referência remota para se comunicar e colaborar entre si para provisionar a solicitação de serviço.

Schoo et al. [14] descreve vários desafios de segurança que afetam o modelo de provisionamento NaaS. Alguns dos desafios de segurança abordados incluem problemas de segurança da informação, ameaças em ambientes de virtualização e segurança de comunicação para redes em nuvem. Posteriormente, Fusenig et al. [13] propuseram uma arquitetura de segurança abstrata para negar os desafios de segurança cobertos em [14]. Eles definiram uma função de conversão de metas de segurança, que se baseia na função de tradução de metas proposta por Bjurling et al. [15] e aprimora isso adicionando funcionalidades de tradução específicas de segurança. O objetivo da função de conversão de meta de segurança é aceitar os requisitos de segurança de várias entidades e produzir soluções ótimas para resolvê-las. Este artigo usa a função de conversão de meta de segurança sugerida por Fusenig et al. [13], mapeia-a para a arquitetura V2C descrita na Seção 3 e a amplia ainda mais integrando três módulos de segurança adicionais. Esses módulos incluem um módulo de autenticação, um módulo de políticas de autorização e controle de acesso e um módulo de garantia. As colocações desses módulos e sua interação com a arquitetura de segurança são mostradas na Figura 3.

4. ARQUITETURA DE SEGURANÇA

O módulo de autenticação desempenha um papel importante no processo de tradução de meta de segurança, pois as metas de segurança fornecidas pelas entidades na infraestrutura V2C exigem uma identificação precisa das entidades envolvidas. A autenticação é realizada não apenas nas entidades, mas também nos recursos físicos / virtuais. Vijaykumar et al. [16] propuseram um algoritmo de gerenciamento de chaves leve e extensível, que pode ser personalizado para o modelo V2C. Uma segunda alternativa é usar um padrão da indústria como o OAuth 2.0 [17,18] para implementar a autenticação.

O módulo de políticas de autorização e controle de acesso define políticas de controle de acesso para cada usuário de automóvel e as implementa durante o processo de alocação de recursos. É importante utilizar modelos de política de controle de acesso que possam ser refletidos até os recursos de rede heterogêneos e, portanto, modelos como o OrBAC [19] não são uma opção viável. Substituições adequadas para um modelo de controle de acesso incluem um modelo ACL [20], ou um modelo MAC / MLS [21, 22,23]. Além disso, o perfil XSPA (Enterprise Security and Privacy Authorization) da XACML (Extensible Access Control Markup Language) [24] pode ser implantado no modelo V2C. O XACML garante que diferentes entidades participantes possam trocar seus atributos e requisitos de privacidade de forma consistente. Isso impediria a ocorrência de diferentes entidades incapazes de intercambiar e compreender os atributos de privacidade devido ao uso de diferentes idiomas para definir e descrever suas políticas de privacidade.

Um módulo de segurança freqüentemente negligenciado é o módulo de garantia, que é responsável por garantir que as diferentes entidades de infraestrutura do modelo V2C estejam em conformidade com os requisitos legais gerais da (s) área (s) operacional (is), requisitos específicos da indústria e serviços. requisitos específicos e requisitos fornecidos pelas diferentes entidades. O módulo de garantia é implantado em toda a arquitetura e correlaciona as ações de gerenciamento com os requisitos desejados.

5. CASOS DE USO

Dois casos de uso podem ser fornecidos pelo modelo V2C para o ecossistema automotivo, ou seja, navegação baseada em nuvem e informações.

Navegação baseada em nuvem

A navegação baseada em nuvem permite que as solicitações de navegação sejam processadas e transmitidas para um usuário de automóvel do provedor de infra-estrutura. O usuário de automóvel tem acesso a uma interface fornecida pelo provedor de infraestrutura, que pode ser usada para inserir solicitações de navegação com restrições específicas. Por exemplo, uma solicitação para evitar rotas com alto congestionamento de tráfego. Cada provedor de infraestrutura (ou um conglomerado de provedores de infraestrutura) pode gerenciar grandes data centers para computar simultaneamente várias rotas, cada uma especificando um subconjunto da solicitação de serviço inserida pelo usuário. A função de tradução de objetivos discutida na Seção 3.2 é empregada para selecionar a melhor rota possível. Esse processo requer o uso simultâneo de várias unidades de processamento. No entanto, o custo geral de provisionamento para o provedor de infraestrutura é amplamente reduzido devido a economias de escala e o serviço é subscrito por um grande número de usuários automobilísticos. Além disso, o provedor de infra-estrutura é capaz de transmitir de forma confiável dados navegacionais de alta qualidade, utilizando os recursos de rede provisionados para o usuário do automóvel.

Uma vantagem proeminente das capacidades aprimoradas de rede é a capacidade de enviar "vistas de rua" de alta definição, além das informações básicas de navegação disponíveis em dispositivos de navegação de última geração instalados em automóveis. O Street View do Google [25] oferece visualizações de rua semelhantes por meio de seus mapas do Google [26], mas o aplicativo não sofreu uma penetração generalizada no mercado em dispositivos de navegação para automóveis. No entanto, as razões para sua baixa penetração variam de baixa largura de banda de rede a fatores operacionais e organizacionais.

Com o modelo V2C proposto neste documento, um serviço de navegação baseado em nuvem pode ser facilmente implantado pelo fabricante do veículo em colaboração com prestadores de serviços / recursos externos. Os provedores de recursos se beneficiarão de economias de escala [27] e terão um baixo OPEX enquanto oferecem os serviços. Por outro lado, os fabricantes de automóveis podem beneficiar-se com a implantação de toda a infra-estrutura de provisionamento de recursos de backbone e obter dois canais de receita sucessivos, ou seja, por meio do usuário de automóvel e do provedor de infraestrutura externa.

Informação baseada em nuvem

A informação baseada em nuvem permite que o usuário de automóvel solicite um serviço de streaming de multimídia através da interface fornecida pelo provedor de infra-estrutura. O (s) provedor (es) da infra-estrutura gerencia (m) uma infraestrutura de backbone e colabora com os provedores de conteúdo externos para provisionar um serviço de streaming de multimídia. Uma gama de serviços de multimídia, seus requisitos de provisionamento, atores envolvidos e análise de negócios são discutidos em [28]. Destes, dois casos de uso importantes para o ecossistema do automóvel são videoconferência e distribuição elástica de vídeo.

A videoconferência é extremamente benéfica se o usuário do automóvel experimentar latência de rede e QoE, com jitter aceitável [29]. Chen et al. [30] propuseram a implementação de redes de retransmissão sem fio ad-hoc sobre veículos em movimento, mas o modelo não fornece fornecimento de rede confiável, seguro, elástico e sob demanda para lidar com rajadas e flutuações de tráfego. Nosso modelo V2C garante melhor QoE ao usuário automotivo, pois integra o NaaS juntamente com os modelos existentes de provisionamento de serviços. Os principais requisitos para distribuição de vídeo são abordados em [31], e o modelo descrito neste documento também garante segurança e entrega confiável para unidades móveis.

6. RESULTADOS E COMPARAÇÃO

Existem três principais arquiteturas e ferramentas de segurança que protegem o (s) modelo (s) de fornecimento de serviços em nuvem backbone, ou seja, arquitetura de computação em nuvem da IBM [32], arquitetura de computação em nuvem do Google [33] e arquitetura de computação em nuvem da Eucalyptus [34]. essas diferentes arquiteturas (de segurança) propostas para o cloud computing com o nosso modelo V2C. Os parâmetros para a comparação são medidos com base na sua relevância para o desempenho, confiabilidade e segurança do nosso modelo. Estes incluem controle de acesso, convergência de rede comutada por pacote e circuito, provisionamento de rede sob demanda, política de acesso baseada em pacote, função de auditoria e garantia, migração de VM com monitoração, plano de abstração de rede de software e segurança multinível.

Em termos de parâmetros de segurança, nosso modelo se comporta razoavelmente bem. Todos os quatro modelos possuem um módulo de controle de acesso e um mecanismo de auditoria e garantia. No entanto, como o nosso modelo está nos estágios iniciais, a segurança em vários níveis não foi incorporada na arquitetura de provisionamento de serviços.

Table 1: Comparison between different architectures

	V2C Model	Google	IBM	Eucalyptus
Controle de acesso	Yes	Yes	Yes	Yes
Convergência de rede por pacotes e circuitos comutados	Yes	-	-	-
Provisionamento de rede sob demanda	Yes	-	-	-
Política de acesso baseada em pacotes	Yes	-	-	-
Função de auditoria e garantia	Yes	Yes	Yes	Yes
Migração de VM com estado	Yes	-	-	-
Lugar de abstração de rede de software	Yes	-	-	-
Segurança multi-nível	-	Yes	Yes	Yes

Por outro lado, nosso modelo se sai melhor em termos de capacidade de rede. É o único modelo que suporta o provisionamento de rede sob demanda, o que melhora a latência e o rendimento da rede. Além disso, a convergência de redes por comutação de pacotes e circuitos [31] integra a comutação de circuitos e pacotes e oferece estabilidade e flexibilidade. Nosso modelo também inclui um plano de abstração de rede de software (representado na Figura 2) e migração de VM com monitoração de estado, o que melhora a flexibilidade e evita travamentos de fornecedores. Finalmente, nosso modelo suporta política de acesso baseada em pacotes [4], que permite ao usuário do automóvel definir diferentes políticas de controle de acesso para diferentes serviços.

7. CONCLUSÃO E TRABALHO FUTURO

Neste documento, foi proposta uma arquitetura de provisionamento de serviços de nuvem segura e personalizada para o ecossistema automotivo, ou seja, V2C. O modelo V2C, com sua arquitetura de segurança totalmente integrada, garante que os recursos solicitados possam ser provisionados de maneira elástica, sob demanda, confiável e segura. Além disso, o documento descreve exemplos de casos de uso para provisionamento de serviços em nuvem em automóveis.

Trabalhos futuros incluem a introdução de um algoritmo de gerenciamento de chaves para suportar o módulo de autenticação e um sistema de detecção de intrusões (baseado em rede e / ou host) para suportar o módulo de garantia.

8. AGRADECIMENTOS

We would like to thank Peter Schoo, Volker Fusenig, and Rajya Deep Dhungana from Fraunhofer AISEC, Munich, Germany for their valuable comments and suggestions regarding the core networking architecture and the automotive ecosystem.

9. REFERÊNCIAS

[1] Lee Badger, Robert Patt-corner, and Jeff Voas. DRAFT Cloud Computing Synopsis and Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 117:84, 2011.

[2] Peter Mell and Timothy Grance. The NIST Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 145(6):7, 2011.

[3] Thomas Edwall. Scalable & Adaptive Internet Solutions (SAIL). Technical report, European Commission's 7^{th} Framework Program, 2011.

[4] Paul Murray. D-5.2 (D-D.1) Cloud Network Architecture Description. Technical report, European Commission's 7^{th} Framework Program, 2011.

[5]K Kaplan. Intel's Smart WiMAX Car - Mobility "Innovision" for Centrino 2, July 2008.

[6]J. Mosyagin. Using 4G wireless technology in the car. In *Transparent Optical Networks (ICTON), 2010 12^{th} International Conference on*, pages 1–4, July 2010.

[7]Weidong Xiang, Yue Huang, and S Majhi. The Design of a Wireless Access for Vehicular Environment (WAVE) prototype for Intelligent Transportation System (ITS) and Vehicular Infrastructure Integration (VII). In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pages 1–2, Sept. 2008.

[8]J. Miller. Fastest path analysis in a Vehicle-to-Infrastructure intelligent transportation system architecture. In *Intelligent Vehicles Symposium, 2009 IEEE*, pages 1125 –1130, June 2009.

[9]M. Torrent-Moreno, J. Mittag, P. Santi, and H Hartenstein. Vehicle-to-Vehicle Communication: Fair Transmit Power Control for Safety-Critical Information. *Vehicular Technology, IEEE Transactions on*, 58(7):3684–3703, Sept. 2009.

[10]Daiheng Ni. Determining traffic-flow characteristics by definition for application in ITS. *Intelligent Transportation Systems, IEEE Transactions on*, 8(2):181–187, June 2007.

[11]N. Seddigh, B. Nandy, R. Makkar, and J.F. Beaumont. Security advances and challenges in 4G wireless networks. In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, pages 62–71, Aug. 2010.

[12] Yu-Hunag Chu, Yao-Ting Chen, Yu-Chieh Chou, and Min-Chi Tseng. A simplified cloud computing network architecture using future internet technologies. In *Network Operations and Management Symposium (APNOMS), 2011 13^{th} Asia-Pacific*, pages 1–4, Sept. 2011.

[13] Volker Fusenig and Ayush Sharma. Security Architecture for Cloud Networking. In *International Conference on Computing, Networking and Communication (ICNC), Maui, Hawaii, USA*, 30^{th}Jan. - 2^{nd} Feb. 2012.

[14] Peter Schoo, Volker Fusenig, Victor Souza, Marcio Melo, Paul Murray, Herve Debar, Houssem Medhioub, and Djamal Zeghlache. Challenges for Cloud Networking Security. In *MONAMI*, pages 298–313, 2010.

[15] Bj ̈orn Bjurling, Rebecca Steinert, and Daniel Gillblad. Translation of probabilistic QoS in hierarchical and decentralized settings. In *APNOMS*, pages 1–8, 2011.

[16]P. Vijayakumar, S. Bose, A. Kannan, and S Siva Subramanian. A Secure Key Distribution Protocol for Multicast Communication. In *Communications in Computer and Information Science*, volume 140, page 249Ű257. Springer, 2011.

[17] Yating Hsu and D. Lee. Authentication and authorization protocol security property analysis with trace inclusion transformation and online minimization. In *Network Protocols (ICNP), 2010 18th IEEE International Conference on*, pages 164 –173, oct. 2010.

[18] Wang Bin, Huang He Yuan, Liu Xiao Xi, and Xu Jing Min. Open Identity Management Framework for SaaS Ecosystem. In *e-Business Engineering, 2009. ICEBE '09. IEEE International Conference on*, pages 512–517, Oct. 2009.

[19]A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, and G Trouessin. Organization Based Access Control. In *4th IEEE International Workshop on Policies for Distributed Systems and Networks (Policy'03)*, June 2003.

[20]J Qian. ACLA: A framework for Access Control List (ACL) Analysis and Optimization. In *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security Issues of the New Century*, pages 4–, Deventer, The Netherlands, The Netherlands, 2001. Kluwer, B.V.

[21]D. Clark and D Wilson. A Comparison of Commercial and Military Computer Security Policies. In *IEEE symposium on security and privacy*, pages 184–194, 1987.

[22] Myong H. Kang, Judith N. Froscher, Brian J. Eppinger, and Ira S. Moskowitz. A Strategy for an MLS Workflow Management System. In *In Proceedings of the 18th IFIP Working Conference on Database Security*, 1999.

[23] Konstantin Knorr. Multilevel Security and Information Flow in Petri Net Workflows. Technical report, In Proceedings of the 9th International Conference on Telecommunication Systems - Modeling and Analysis, Special Session on Security Aspects of Telecommunication Systems, 2001.

[24] Bill Parducci, Hal Lockhart, and Erik Rissanen. XACML v3.0 Privacy Policy Profile Version 1.0. *Policy*, pages 1–11, August 2010.

[25] Amir Roshan Zamir and Mubarak Shah. Accurate Image Localization Based on Google Maps Street View], booktitle = Proceedings of the European Conference on Computer Vision (ECCV. 2010.

[26] Christopher C Miller. A Beast in the Field: The Google Maps Mashup as GIS/2. *Cartographica The International Journal for Geographic Information and Geovisualization*, 41(3):187–199, 2006.

[27] Joseph Berechman and Genevieve Giuliano. Economies of scale in bus transit: A review of concepts and evidence. *Transportation*, 12:313–332, 1985. 10.1007/BF00165470.

[28]T. Lev ä, J. Gonçalves, and R. J. Ferreira. Description of project wide scenarios and use cases. Technical Report FP7-ICT-2009-5-257448-SAIL/D2.1, European Commission's 7th Framework Program, http://www.sail-project.eu/wp-content/uploads/2011/09/SAIL DA1 v1 2_final.pdf, 2009.

[29] IEEE Standard for Measurement of Video Jitter and Wander. *IEEE Std 1521-2003*, pages c1–14, 14 2009.

[30] Zong Da Chen, H.T. Kung, and Dario Vlah. Ad hoc relay wireless networks over moving vehicles on highways. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '01, pages 247–250, New York, NY, USA, 2001. ACM.

[31] Thomas Edwall. Description of project wide scenarios and use cases. Technical report, European Commission's 7th Framework Program, 2011.

[32]B Schmidt-Wesche, Brian Snitzer, Gerd Breiter, Gerhard Widmayer, Jim Whitmore, Julissa Villareal, Michael Behrendt, R Caponigro, R Chang, S Pappe, and Et Al. IBM Cloud Computing & Common Cloud Management Platform Reference Architecture (CC & CCMP RA) 1.0, 2010.

[33]J I A Xiaojing. Google Cloud Computing Platform Technology Architecture and the Impact of Its Cost. *2010 Second World Congress on Software Engineering*, (70801067):17–20, 2010.

[34]Eucalyptus Systems. Eucalyptus Systems Eucalyptus Open-Source Cloud Computing Infrastructure - An Overview Eucalyptus Systems An Overview. *Technology*, 180:012051, August 2009.