Fog computing texnologiyalarında məlumatların təhlükəsizliyi məsələləri

Rəşid Ələkbərov[1], Məmməd Həşimov[2]
[1,2] AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*t.direktor_muavini@iit.science.az*, [2]*mamedhashimov@gmail.com*

***Xülasə*— Məqalədə Əşyaların İnternetində (IoT) Fog Computing texnologiyalarından istifadənin perspektivləri göstərilmişdir. Bu texnologiyadan istifadə zamanı məlumatların təhlükəsizliyi məsələləri analiz edilmişdir. Fog computingin müxtəlif səviyyələrində potensial təhlükəsizlik təhdidləri təhlil edilmiş və həmin təhdidlər nəticəsində məlumatların məxfiliyinə təsir edən müəyyən aspektlər qeyd olunmuşdur.**

Açar sözlər— əşyaların interneti; hesablama buludları; duman texnologiyaları; duman təhlükəsizliyi

I. GİRİŞ

Əşyaların İnterneti *(ing. İnternet of things, IoT),* Kiber-Fiziki sistemlər və Mobil İnternet texnologiyalarının inkişafı, insan, maşın və əşyalar da daxil olmaqla müxtəlif obyektləri istənilən zaman istənilən məkanda informasiya mühiti ilə əlaqələndirir. "Əşyaların İnterneti" Dünya İqtisadi Forumunun qiymətləndirməsində dünyanı dəyişdirəcək texnologiyalar arasında ilk sıralarda yer alır və bu texnologiyaların yaxın 10 ildə dünya iqtisadiyyatında əsas trend olacağı proqnozlaşdırılır. IoT cihazlarının sayı 2017-ci ildə 31% artaraq 8.4 milyarda çatmış və 2020-ci ildə bu sayın 30 milyarda çatacağı gözlənilir [1]. Misli görünməmiş həcmdə və növdə verilənlər generasiya edilir. Bu isə öz növbəsində "məlumat partlayışı" adlanan böyük miqdarda verilənlərin yaranmasına gətirib çıxarmışdır. Məlumatların həcmində müşahidə edilən sürətli artım ilə bərabər məlumatların generasiya sürəti də getdikcə artmaqdadır. Bu isə böyük həcmdə məlumatların emalı və saxlama imkanlarının müasir dövrdə tələblərə cavab verə bilmədiyini göstərir.

IoT texnologiyalarında istifadə edilən ağıllı cihazların hesablama gücü, batareya, yaddaş və s. məhdud olduğundan, IoT proqramları və xidmətləri çox vaxt buludda yerləşən güclü server tərəfindən təmin edilir. Belə ki, cloud computing, son istifadəçilərə xidmətlərin göstərilməsi və tətbiqləri aşağı xərclə çoxsaylı resurslarla təmin etmək üçün perspektivli həll hesab edilir [2]. Beləliklə, yüksək hesablama gücünə və yaddaş imkanlarına malik cloud computing həmin məlumatların emalı üçün effektiv həll kimi qəbul olunur.

Cloud computing mərkəzləşdirilmiş bir hesablama modeli olduğundan, hesablamaların əksəriyyəti buludda yerinə yetirilir. Bu isə, bütün məlumat və sorğuların mərkəzləşdirilmiş buluda ötürülməsi deməkdir. Verilənlərin emal sürətinin artmasına baxmayaraq, şəbəkənin keçiriciliyi əhəmiyyətli dərəcədə artmamışdır. Beləliklə, şəbəkənin keçiriciliyi böyük həcmdə məlumatların emal edilməsi üçün cloud computing sistemi üçün problemlər yaradır [3].

Cloud computing-in generasiya olunmuş məlumatların emal edilib saxlanılması üçün effektiv texnologiya olmasına baxmayaraq, mövcud tətbiqlərin real zamanda istifadəsi və ya gecikmə ilə bağlı problemlərə malik olması, eyni zamanda şəbəkənin aşağı keçiricilik qabiliyyəti kimi problemlərin həlli yalnız cloud computing vasitəsilə mümkün deyil.

Yuxarıda deyilənləri nəzərə alaraq hal-hazırda məlumatların toplanması (sensorlardan) və ilkin emalı üçün aralıq hesablama sistemlərindən geniş istifadə olunur. Bu səbəbdən də hesablama buludlarından əlavə fog computing ("hesablama dumanı") adlanan yeni hesablama paradiqması təklif edilmişdir.

II. FOG COMPUTİNG TEXNOLOGİYALARI

Fog texnologiyaları IoT-a adekvat həll gətirən yeni konsepsiyadır. Ənənəvi cloud computing sistemində verilənlər mərkəzinin yükünün azaldılması üçün fog computing coğrafi olaraq paylanmış, gecikmə problemli və yüksək keyfiyyətli xidmət təmin edən IoT tətbiqlərinin dəstəklənməsi üçün alternativ həll kimi təklif edilmişdir.

Fog computing sistemi ilk dəfə Cisco şirkəti tərəfindən təklif edilmişdir. "Duman" termini "*yerə ən yaxın bulud*" kimi təklif edilmişdir, yəni yenilənmiş və daha yaxşı tətbiq və ya xidmətləri təmin edə bilən mərkəzdən (nüvədən) hüdudlaradək hesablama kimi izah olunur. Fog computing – son istifadəçi ilə data mərkəz arasında hesablama, yaddaş və şəbəkə xidmətlərini təmin edən yüksək səviyyədə virtuallaşdırılmış platformadır [4].

Fog computing ümumiyyətlə cloud computing ilə əlaqələndirilir. Məsələn, hesablama, yaddaş və şəbəkə resursları həm fog computing, həm də cloud computingin struktur bloklarıdır. Bu isə onu göstərir ki, əksər cloud computing texnologiyaları fog computing texnologiyalarına birbaşa tətbiq oluna bilər. Bununla yanaşı, fog computing sistemi onu digər mövcud hesablama arxitekturalarından fərqləndirən bir sıra unikal xüsusiyyətlərə malikdir. Həmin xüsusiyyətlərdən biri və ən əhəmiyyətlisi onun son istifadəçilərə yaxın məsafədə yerləşməsidir [2].

Fog computing qovşaqları sensor və kənar qurğuların generasiya etdiyi məlumatları emal edir və saxlayır. Daha sonra isə qalan əhəmiyyətli məlumatların saxlanılması və ya gələcəkdə emal edilmə üçün bulud serverinə ötürülür. Ənənəvi cloud computing modeli ilə birləşərək, fog computing cloud computingə daha səmərəli xidmət göstərməyə imkan yaradır.

DOI: 10.25045/NCInfoSec.2019.38

IoT-da Fog computing texnologiyalarından istifadənin üstünlükləri [5]:

- Bulud xidmətləri fog computing vasitəsilə IoT cihazları üçün təmin olunur;
- Fog computing, cloud computing ilə IoT cihazları arasındakı səviyyəni təşkil edir;
- Fog computingdə bir neçə qovşaq mövcud ola bilər;
- Sensorlar vasitəsilə toplanan məlumatlar buluda göndərilmədən əvvəl fog serverlərdə emal edilir;
- Fog computing gecikməni azaldır, buludun ötürücülük və yaddaş resurslarına qənaət etməyə imkan verir.

Fog texnologiyası əsasən aşağıdakı sahələrdə tətbiq edilir [6]:

- Ağıllı şəhərlərdə (nəqliyyatda işıqlandırma sistemi);
- Real zamanda sağlamlığın təhlili (xronik xəstəliyi olan xəstələr real zamanla izlənilə bilər, fövqəladə hallarda müvafiq həkimlərə dərhal xəbərdarlıq göndərilməsi və s.);
- Enerji səmərəli intellektual sistem (gündəlik enerji istehlakı hesabatlarını hazırlayır, daha qənaətli enerji istifadəsi planını təklif edir və s.);
- Real zamanda dəmiryolunun monitorinqi (yol şəraitinin real zamanda monitorinqi);
- Real zamanda külək dəyirmanı və turbinin təhlili (küləyin istiqaməti və sürətinin analizi) və s.

Son illərdə cloud computing, fog computing kimi korporativ idarəetmə sistemlərinə keçid müşahidə olunur. Neft-qaz sənayesində SCADA kimi tətbiqlərin fog mühitinə köçürülməsi, potensial xərclərin azaldılması, miqyaslanma imkanları, səmərəli sistem konfiqurasiyası və texniki təminatı baxımından daha cəlbedici hesab olunur [7]. Neft-qaz sənayesi üçün fog texnologiyası əsasən aşağıdakı sahələrdə tətbiq edilir:

- Neft-qaz sənayesində boru kəmərinin optimallaşdırılması (təzyiqin, axının, kompressorun real zamanda monitorinqi);
- Neft quyularının qazma qurğularına nəzarət (neft pompalarının enerji təchizatı gərginliyinə və cərəyanına nəzarət);
- Geolokasiya vasitəsilə heyətin izlənməsi və müəyyən təhlükəsizlik amillərinin monitorinqi və s.

IoT texnologiyaları vasitəsilə əlaqələndirilən obyektlərin sayı sürətlə artdığından böyük həcmdə məlumatlar generasiya edilir. Verilənləri generasiya edən qovşaqlar paylanmış olduğundan onlara mərkəzləşmiş nəzarət çətinləşir. Digər vacib məsələlərdən biri isə paylanmış Fog computing arxitekturasındakı verilənlərin təhlükəsizliyi və məxfiliyidir.

III. FOG COMPUTİNG TEXNOLOGİYALARINDA TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Fog computing, məlumat mərkəzinin ümumi yükünün azaldılması məqsədilə paylanmış qovşaqların hesablama gücünə əsaslanır. Bundan əlavə, duman qovşaqları böyük coğrafi ərazilərə səpələndiyindən müxtəlif şəbəkə standartları, protokolları, topologiyalarından və s. istifadə olunur. Duman qovşaqları arasındakı rabitə əlaqəsindən aşağıdakı təhlükəsizlik və etibarlılıq məsələləri meydana çıxmışdır [8]:

- Hər duman qovşağı müstəqil olub, mesaj ötürmə yolu ilə digərləri ilə əməkdaşlıq edə bilir. Duman qovşaqları şəbəkəyə yaxşı inteqrasiya edilmədikdə və birlikdə qənaətbəxş xidmətləri təmin edə bilmədikdə etibarlılıq problemləri yarana bilər.
- Duman qovşaqları istənilən şəbəkə vasitəsilə əlaqə qura bilər. Onlar arasındakı rabitə çox böyük ola bilər. Gecikmə problemli tətbiqlər üçün bu, ciddi bir problem ola bilər. Bu, sistemin etibarlılığını aşağı sala, daha sonra isə tapşırığın həlli müddəti başa çatdıqda istifadəçilər arasında etibar böhranına səbəb ola bilər. Nəticədə, yerüstü rabitənin tələb edilən səviyyəyə endirilməsi vacib məsələyə çevrilir.
- Yeni duman qovşağı əlavə edildikdə və ya əvvəlki qovşaq xidməti təmin edə bilmədikdə və şəbəkədən çıxarılmalı olduqda, digər duman qovşaqları aralarındakı rabitəni təmin etmək məqsədilə potensial olaraq öz topologiyalarını dəyişdirməli və rabitə strukturlarını yenidən qurmalı olurlar. Topologiyanın yenidən qurulması prosesi isə yeni təhlükəsizlik problemlərinin yaranmasına səbəb olur.
- Duman qovşaqları digər qovşaqlarla əməkdaşlıq etdiyi zaman, hər hansı qovşaq zərərli istifadəçi tərəfindən hücuma məruz qaldıqda və yoluxdurulduqda, yoluxmuş qovşağın özü digər qovşaqlara hücum edə və ya onları da yoluxdura bilər. Bu isə, bütün əlaqəli qovşaqlar arasında təhlükəsizlik və ya inam böhranına səbəb ola bilər.

Fog computing platformasının yaradılma mərhələlərinin hər birində təhlükəsizlik və məxfilik nəzərə alınmalıdır. Bu, fog computing sahəsində mövcud olan ən problemli məsələlərdən biri hesab olunur. Fog computing texnologiyasının müxtəlif səviyyələrində potensial təhlükəsizlik təhdidlərinə aşağıdakıları aid etmək olar [9, 10, 11]:

- **Qovşaqların aşkarlanması/Cihazlara müdaxilə (Node Capture/Device Tampering):** IoT-un şəbəkə keçidlərində mövcud olan obyektlərə (əşyalara) müdaxilə etməklə vacib məlumatların sızması baş verir. Bu isə bütün şəbəkədəki istifadəçi məlumatlarının məxfiliyini təhlükə altına atır.
- **Aldadıcı hücumlar (Spoofing Attack):** Hücum edən məlumatları saxtalaşdıraraq onları şəbəkəyə göndərir. İoT qurğuları orijinal mənbənin saxta

identifikasiyalarını qəbul edərək hücum edən üçün sistemə tam girişi təmin edir.

- **Zərərli məlumatlar (Malicious Data):** Sistemə əlavə olunduqda zərərli qovşaq zərərli məlumat yaymaqla bütün sistemi yoluxdurur (pozur).
- **Təkrar hücumlar (Replay Attack):** Orijinal məlumat paketləri saxta məlumat paketləri ilə əvəz olunaraq şəbəkənin etibarlı identifikasiyası təhlükə altına alınır.
- **SYBIL hücumu:** Zərərli qovşağın şəbəkəyə daxil olması nəticəsində aqreqat mesajı saxta mesajla dəyişdirilir. Ən effektiv bağlantının seçilməsi imkanı bloklanır.
- **Selektiv yönləndirmə (Selective Forwarding):** Bəzi məlumat paketləri bloklanır və zərərli qovşaq tərəfindən selektiv şəkildə atılır. Selektiv yönləndirmə hücumlarının əsas iki növü mövcuddur. Bunlara məlumat paketlərinin atılması və məlumat paketlərinin yoluxmuş qovşaq tərəfindən təsadüfi olaraq yönləndirilməsi aiddir.
- **Qara dəlik hücumu (Blackhole Attack):** Etibarsız marşrutlaşdırma məlumatı yaradılır və bütün məlumat paketləri “qara dəliyə” yönəldirilir. Bu, şəbəkənin həddən artıq yüklənməsinə və paketin atılmasına səbəb ola bilər.
- **Hello-Flood Hücumu:** Hücum edən, şəbəkə tıxacı yaratmaq məqsədilə kanalı saxta məlumat paketləri ilə yükləyir. Bundan əlavə, o, məlumat paketinin ötürülməsində iştirak etmək məqsədilə hər bir qovşağı ona qonşu olan qovşağın zərərli olduğuna inandırır.
- **Acknowledge Flooding:** DoS (Deniel-of-service attacks (Xidmətdən imtina hücumları)) hücumarında olduğu kimi, hücum edən təsdiqlənmədən istifadə etməklə qonşu qovşaqlara saxta məlumatlar göndərir.
- **Məlumatın aşkarlanması (Data Disclosure):** Hücum edən, qovşaqdan məlumatı əldə etmək məqsədilə verilənlərin axtarış metodlarından istifadə edir, bu isə məxfilik təhdidlərinə səbəb ola bilər.
- **Sniffer/Casus (Sniffer/Logger):** Hücum edən, trafik analizatorundan (sniffering) istifadə etməklə şifrə, e-poçt və FTP faylları kimi vacib məlumatları ələ keçirir. Şəbəkədəki bir çox protokollar trafik analizatoruna qarşı davamlı deyil.
- **Fişinq hücumu (Phishing attack):** Vacib məlumatların ələ keçirilməsi və məhv edilməsi üçün əsas orqanın e-poçt ünvanından istifadə olunur. Burada hücum edən virusla yoluxmuş e-poçt və fişinq veb saytları vasitəsilə istifadəçilərin identifikasiya məlumatlarını saxtalaşdırmaqla, onların gizli məlumatlarını (şəxsiyyət, parol) ələ keçirə bilər.
- **İnyeksiya (Injection):** Serverdə icra olunan proqrama zərərli kodların yeridilməsindən ibarət olub ən çox istifadə edilən hücumlardan biridir. Bu hücum, məlumatlar itkisinə səbəb ola və proqramın hesabatlılığına ziyan vura bilər
- **Seansın oğurlanması hücumu (Session Hijacking):** Bu hücum əsasən digər şəxsin kimliyinə hücumdan ibarətdir. Bununla da, autentifikasiya məlumatlarının idarəetməsində yaranan boşluqlar səbəbindən hücum edən fərdi kimlikləri əldə etmək imkanı qazanır.
- **Məlumat məxfiliyi:** Məlumatların qorunma üsullarının zəif olması, məlumat itkisi və sistemə uzunmüddətli ziyanın vurulması ilə nəticələnir.

Müxtəlif heterogen İOT cihazları ilə birgə paylanmış fog computing sistemi, müxtəlif təhlükəsizlik hücumlarına qarşı həssasdır. İstifadəçi məlumatları duman qovşaqları üzərindən toplandığı, emal edildiyi, ötürüldüyü və paylandığı üçün onların məxfiliyi bir çox baxımdan fog computing sahəsində ciddi məsələlərdən birinə çevrilmişdir. Hücum edən, təhlükəsizliyi zəif təmin olunmuş kənar qovşaqlardan giriş nöqtəsi kimi istifadə edə bilər. Şəbəkəyə daxil olmuş şəxs isə istifadəçilər arasında mübadilə edilən məxfi məlumatları mənimsəyə və oğurlaya bilər. Heç bir istifadəçi məlumatlarının və ya kimliyinin açıqlanmasını istəmir. Lakin təhdid və ya hücumlar nəticəsində məlumatların qorunub saxlanması mümkün deyil. İstifadəçi məxfiliyinə aşağıdakı bəndlər aiddir [12,13]:

- **Kimliyin məxfiliyi**. İstifadəçi kimliyinə obyektin əsas atributları, yəni onun adı, mobil telefon nömrəsi, ev ünvanı, viza eyniləşdirmə nömrəsi, lisenziya eyniləşdirmə nömrəsi daxildir. Bütün bu məlumatları qeyd etməklə duman qovşaqlarının identifikasiyasını əldə etmək mümkündür.
- **Verilənlərin məxfiliyi** duman qovşaqları vasitəsilə əlaqə qurarkən istifadəçi məlumatları kənar şəxslərin əlinə düşə bilər. Həmin məlumatları araşdırmaqla, istifadəçinin ünvanı, üstünlük verdiyi ideyalar və siyasi ideologiya kimi müxtəlif növ əhəmiyyətli məlumatlar əldə edilə bilər. Məsələn, onlayn səsvermə, istifadəçinin siyasi fikirlərinin aşkarlanmasına səbəb ola bilər.
- **İstifadə məxfiliyi** dedikdə, adətən, istifadəçinin duman xidmətlərindən istifadə etdiyi prinsip və ya qaydalar nəzərdə tutulur. Məsələn, ağıllı sayğacın qeydə aldığı məlumatlar istifadəçilərin yatmaq vaxtını və ya evdə olmadığı vaxtı aşkarlamağa imkan verir, bununla da onun məxfiliyi pozulur.
- **Yerləşmə məxfiliyi** adətən fog computing texnologiyasının hüdudlarında yerləşən istifadəçilərin yerləşmə məxfiliyinə aid olur. Məlumatlar adətən son duman qovşaqlarına çatdırıldığından istifadəçilərin digər duman qovşaqlarından hansı məsafədə yerləşdiyini təyin etmək tələb oluna bilər. Bundan

əlavə, istifadəçi bir çox duman xidmətlərindən istifadə etdiyi halda, məlumatların hansı yolla əldə edildiyi asanlıqla təyin edilə bilər və bu səbəbdən də yerləşmə məxfiliyi təhlükə altına düşər. Ümumiyyətlə, fog computing istifadəçisi üçün ən yaxın duman qovşağı seçilir. Bu seçim istifadəçinin yük balansı, statusu, gecikməsi və s. kimi meyarlar əsasında həyata keçirilir. Yerləşmə haqqında məlumatın əlyetərliliyi hər iki tərəf – həm istifadəçi, həm də duman qovşaqları üçün təhlükəli ola bilər. İstənilən duman qovşağından son istifadəçinin yeri, son istifadəçidən isə duman qovşağının yeri asanlıqla təyin edilə bilər.

NƏTİCƏ

Əşyaların İnterneti texnologiyalarının yaradılması, müasir dövrdə istənilən yerdə rast gəlinən avadanlıqlar arasında qarşılıqlı əlaqə və kommunikasiyaya səbəb olmuşdur. Son dövrlərdə müxtəlif təyinatlı sensorlar vasitəsilə toplanan məlumatların emal edilib saxlanılması üçün Fog Computing texnologiyalarından istifadə olunması daha səmərəli hesab olunur. Cloud computinglə müqayisədə Fog computing, paylanmış qovşaqların hesablama gücünə əsaslanır. Bu səbəbdən də Fog computing texnologiyasında təhlükəsizliyin təmin olunması daha mürəkkəbdir. Bu məqsədlə də, məqalədə Fog computing şəbəkəsində məlumatların məxfiliyinə təsir edən potensial təhlükəsizlik təhdidləri analiz olunmuşdur.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikası Dövlət Neft Şirkətinin (SOCAR) Elm Fondunun mailyyə yardımı ilə yerinə yetirilmişdir – **Müqavilə № 03LR – AMEA.**

İSTİNADLAR

[1] Report-internet of things. http://reports.weforum.org/industrial-internet-of-things/generalfindings/2-1-the-state-of-the-market/

[2] S. Yi, Z. Hao, Z. Qin, Q. Li, “Fog Computing: Platform and Applications,” Third IEEE Workshop on Hot Topics in Web Systems and Technologies, pp. 73-78, 2015.

[3] P. Hu, S. Dhelima, H. Ning, T. Qiu, “Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues,” Journal of Network and Computer Applications, vol. 98, pp. 27-42,2017

[4] M. Mukherjee, L. Shu, D. Wang, “Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges,” IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1826-1857, 2018

[5] H.F. Atlam, R.J. Walters, G.B. Wills, “Fog Computing and the Internet of Things: A Review,” Big Data Cognitive Computing Journal, vol. 2, no. 2, 2018.

[6] A.V. Dastjerdi, H.Gupta, R.N. Calheiros, S.K. Ghosh, R. Buyya, "Fog Computing: principles, architectures, and applications,” Internet of Things: Principles and Paradigms, Chapter 4, pp. 61-75, 2016

[7] M. D. Stojanović, S. V. B. Rakas, J. D. M.Petrović, ‘Scada Systems in the Cloud and Fog Environments: Migration Scenarios and Security Issues,” Electronics and Energetics, vol. 32, no. 3, pp. 345-358, 2019.

[8] P.Y. Zhang, M. C. Zhou, G. Fortino, “Security and trust issues in Fog computing: A survey,” Future Generation Computer Systems, vol. 88, pp. 16-27, 2018

[9] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, R. Ranjan, “Fog Computing Security Challenges and Future Directions [Energy and Security],” IEEE Consumer Electronics Magazine, vol. 8, no. 3, pp. 92-96, 2019.

[10] T. Veerraju, K. K. Kumar, “A survey on fog computing: research challenges in security and privacy issues,” International Journal of Engineering & Technology, vol. 7, pp. 335-340, 2018

[11] D. Puthal, S. Nepal, R. Ranjan, J, Chen, “Threats to Networking Cloud and Edge Datacenters in the Internet of Things,” IEEE Cloud Computing, vol. 3, no. 3, pp. 64-71, 2016

[12] A. Aljumah, T. A. Ahanger, “Fog Computing and Security Issues: A review,” 7th International Conference on Computers Communications and Control (ICCCC), pp. 237-239, 2018

[13] P. Kumar, N. Zaidi, T, Choudhur, “Fog Computing: Common Security Issues and Proposed Countermeasures,” 5th International Conference on System Modeling &Advancement in Research Trends, pp. 311-315, 2016

DATA SECURITY IN FOG COMPUTING

Rashid Alekperov[1], Mammad Hashimov[2]

[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]*t.direktor_muavini@iit.science.az,*
[2]*mamedhashimov@gmail.com*

Abstract— The article highlights the prospects of using fog computing in the Internet of Things. The use of this technology is analyzed for data security. Potential security threats at various levels of Fog Computing are analyzed. Some aspects caused by these threats affecting data privacy are identified.

Keywords— *Internet of Things, Cloud computing, Fog computing, Fog security*