DOI: 10.34185/1991-7848.itmm.2025.01.090

ВИКОРИСТАННЯ МОДЕЛІ НА ОСНОВИ БЕЗПЕКИ ДЛЯ ЗАХИСТУ ХМАРНИХ СЕРЕДОВИЩ

Бобренок В.В.[1], Гуда І.А.[2]

[1] Дніпровський металургійний інститут Українського державного університету науки і технологій, аспірант, Україна

[2]Дніпровський металургійний інститут Українського державного університету науки і технологій, докт. техн. наук, проф., Україна

Анотація. *Стрімкий ріст популярності хмарних середовищ вимагає приділяти особливу увагу безпеці ресурсів та даних, розташованих у хмарі. Розглянута концепція довіри та її властивості, завдяки яким вона може бути використана для опису взаємодії компонентів у хмарних середовищах. Завдяки цьому моделі на її основі можуть бути застосовані для захисту цих середовищ. Розглянуті реалізації подібних моделей, а саме: TNA-SL, InterTrust, ODTMF, Fuzz Art та їх модифікації. Були визначені вимоги до них, відомі недоліки та переваги. Як результат, був зроблений висновок, що моделі на основі довіри можуть бути використані для захисту хмарних середовищ, проте вони потребують оптимізацій як часу виконання, так і масштабування для подальшого використання. Також було визначено, що варто звернути увагу на їх використання у об'єднаних хмарних середовищах.*

Ключові слова: *хмарні середовища, хмарні обчислення, розподілені системи, кібербезпека, захист інформації, моделі на основі довіри.*

Хмарні середовища пропонують доступ до масштабованих обчислювальних ресурсів за запитом через Інтернет. Можливості, які це надає, занадто привабливі для споживачів, щоб їх ігнорувати. Однак парадигма хмарних обчислень також має недоліки, зокрема їх непрозорий характер, що призводить до значних проблем щодо довіри та безпеки, які перешкоджають їх розвитку та поширенню. Щоб виправити це, розробляється модель оцінки та керування довірою.

По суті, довіра означає віру в здатність суб'єкта діяти певним чином у конкретному контексті [1]. Довіра, як показник, має декілька важливих властивостей:

- Довіра залежить від прямої взаємодії, спостереження або досвіду між компонентами системи.

- Компоненти системи можуть не мати історії попередніх взаємодій, однак вони можуть використовувати дані від інших об'єктів. Йдеться мова про транзитивну довіру.
- Показник довіри залежить від конкретної пари компонентів системи, на яких зосереджено увагу, і змінюється від однієї пари до іншої.
- Різні компоненти системи можуть мати різний ступінь довіри один до одного. Насправді, те, що об’єкт А довіряє об’єкту В, не означає, що об’єкт В повинен довіряти об’єкту А.
- Довіра – це за своєю суттю суб’єктивний показник, який базується на різних властивостях або доказах, і деякі з них можуть мати більшу вагу, ніж інші.
- Довіра – контекстно-залежна ознака: довіра «А» до «В» відрізняється в залежності від контексту.
- Довіра фактично є сумішшю деяких індивідуальних характеристик: правдивість, чесність, надійність, компетентність, безпека та своєчасність.
- Довіра залежить від історії: вона використовує попередній досвід, який може вплинути на поточний ступінь довіри.
- Довіра є динамічним показником, що змінюється з часом. Це дає змогу відповідати змінам у системі.

Іншим важливим аспектом є поширення довіри, що полягає в тому, як поширювати показники довіри у системі. Загалом, механізми поширення довіри поділяються на розподілені та централізовані.

- Розподілений метод: компоненти системи поширюють показники довіри без використання централізованого брокеру. Адміністрування такого розповсюдження є складним, але робить можливим подальше масштабування.
- Централізований метод: для цього методу потрібен окремий компонент системи, що буде зберігати показники довіри та надавати іншим учасникам доступ до них.

Перераховані властивості довіри роблять можливим використання моделей на її основі для захисту даних та обчислювальних ресурсів. Так алгоритм TNA-SL [2] є добре відомим алгоритмом керування довірою у P2P мережах. Цей алгоритм представляє довірчу мережу між одноранговими вузлами як спрямований послідовний паралельний граф (DSPG) без циклу, що запобігає створенню кількох шляхів між кожною парою однорангових вузлів. Спрощення графіків і визначення довіри базуються на суб’єктивній логіці, згідно з якою думки кожного учасника системи про інших вимірюються та зберігаються. Сила цього алгоритму полягає в точності інформації про довіру та чіткому визначенні негативної довіри. Відомі недоліки цього алгоритму

включають його тривалий час виконання через часте множення матриць, необхідне для визначення місцезнаходження довіреного однорангового пристрою, втрату деякої довірчої інформації для уникнення циклів на графіку та обмежену масштабованість мережі. У [3] вводиться розширена суб’єктивна логіка для управління довірою (ESL-TM) у P2P мережах. Це передбачає новий фактор довіри – фактор занепаду – який використовується як частина механізму покарання після транзакції з негативним рейтингом. У роботі [4] представлено алгоритм InterTrust як потенційний інструмент для управління довірою в об’єднаних хмарних середовищах, який покращує алгоритм TNA-SL, зокрема з точки зору масштабованості та часу виконання. Ця модифікація робить алгоритм TNA-SL більш придатним у випадку об’єднаних хмарних середовищах. Алгоритм InterTrust усуває складність, з точки зору виконання та простору, пов’язану з двома матрицями n × n, які потрібні для алгоритму TNA-SL. Крім того, InterTrust кумулятивно зберігає всю попередню інформацію про довіру між одноранговими вузлами, щоб подолати втрату інформації про довіру в оригінальному алгоритмі.

Інший алгоритм, заснований на розширеній суб'єктивній логіці, запропоновано в [1]. Модель довіри домену організації для федерацій (ODTMF) має на меті оцінити значення довіри доменів організації за допомогою нового оператора, який називається оператором ваги, щоб показати різний вплив кожного учасника федерації організації.

Спеціально для хмар Hadoop [5,6] було розроблено систему управління довірою в [7,8]. Для досягнення високої масштабованості всі обчислення довіри формулюються та виконуються як розподілені хмарні обчислення. Такі параметри, як час ініціації, ціна, швидкість обробки, частота помилок і пропускна здатність, використовуються для розрахунку значень довіри, які періодично оновлюються, щоб гарантувати, що довірені ресурси можуть бути призначені користувачам з вищими значеннями довіри.

У [9] модель довіри на основі домену представлена в рамках хмарної безпеки. Основна увага зосереджена на фільтрації ненадійного зворотного зв’язку довіри, щоб зробити системи більш надійними. Техніка нечіткої логіки

під назвою Fuzzy ART запропонована в [40], яка використовує довіру віртуальних машин у хмарних середовищах.

Висновки. Концепт довіри завдяки своїм властивостям дозволяє описувати взаємодію компонентів у хмарних середовищах, що за своєю природою є дуже динамічними. Завдяки цьому моделі на основі довіри можуть бути використані для захисту хмарних середовищ. Проте для цього необхідно вирішити проблеми розрахунку показника довіри а також його поширення у системі. Наведені спроби реалізації даної моделі значно збільшують час відповіді у системі, або ж є доволі спеціалізованими [5,6,7,8], що робить їх використання неможливим у загальному випадку. Також варто приділити окрему увагу об'єднаним хмарним середовищам, використання яких може ускладнити вирішення поставлених задач, проте може зробити модель кориснішою для користувачів.

ЛІТЕРАТУРА

1. Hu Z, Liu L, Wang C (2011) Organization domain trust evaluation model in federated environment based on subjective logic. In: International conference on information technology, computer engineering and management sciences (ICM). IEEE, Nanjing, Jiangsu, China, pp 380-384
2. Jøsang A, Bhuiyan T (2008) Optimal trust network analysis with subjective logic. In: 2nd International conference on emerging security information, systems and technologies. IEEE, Cap Esterel, France, pp 179-184
3. Ma X, Wang Z, Liu F, Bian J (2010) A trust model based on the extended subjective logic for P2P networks. In: 2nd International conference on e-business and information system security. IEEE, Wuhan, China, pp 1-4
4. Kurdi, H., Alfaries, A., Al-Anazi, A. et al. A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. J Supercomput 75, 3534–3554 (2019). https://doi.org/10.1007/s11227-018-2669-y
5. Shvachko K, Kuang H, Radia S, Chansler R (2010) The hadoop distributed file system. In: 26th Symposium on mass storage systems and technologies (MSST). IEEE, Incline Village, NV, USA, pp 1-10
6. Rao S, Wang Y, Tao XL (2010) The comprehensive trust model in P2P based on improved eigentrust algorithm. In: International conference on measuring technology and mechatronics automation. IEEE, Changsha City, China, pp 822-825
7. Khan SM, Hamlen KW (2012) Hatman: intra-cloud trust management for hadoop. In: 5th International conference on cloud computing. IEEE, Honolulu, HI, USA, pp 494-501

8. Nishikawa T, Fujita S (2010) An effective risk avoidance scheme for the eigentrust reputation management system. In: 1st International conference on networking and computing. IEEE, Higashi-Hiroshima, Japan, pp 36-43
9. Abrams Z, Mcgrew R, Plotkin S (2005) A non-manipulable trust system based on EigenTrust. ACM SIGecom Exch 5:21-30
10. Jaiganesh M, Aarthi M, & Kumar AVA (2015) Fuzzy ART-Based User Behavior Trust in Cloud Computing. in Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Eds.New Delhi: Springer:341-348.

TRUST BASED MODEL FOR CLOUD SECURITY

Viacheslav Bobrenok, Anton Guda

Abstract. *The rapid growth in the popularity of cloud environments requires special attention to be paid to the security of resources and data located in the cloud. The concept of trust and its properties, thanks to which it can be used to describe the interaction of components in cloud environments, are considered. Due to this, models based on this concept can be used to protect these cloud environments. Implementations of such models, namely: TNA-SL, InterTrust, ODTMF, Fuzz Art and their modifications, were considered. Requirements for them were determined, disadvantages and advantages were known. As a result, it was concluded that trust-based models can be used to protect cloud environments, but they require optimizations of both execution time and scalability for further use. It was also determined that it is worth paying attention to their use in federated cloud environments.*

Keywords: *cloud environments, cloud computing, distributed systems, cybersecurity, data security, trust based models*

REFERENCES

1. Hu Z, Liu L, Wang C (2011) Organization domain trust evaluation model in federated environment based on subjective logic. In: International conference on information technology, computer engineering and management sciences (ICM). IEEE, Nanjing, Jiangsu, China, pp 380-384
2. Jøsang A, Bhuiyan T (2008) Optimal trust network analysis with subjective logic. In: 2nd International conference on emerging security information, systems and technologies. IEEE, Cap Esterel, France, pp 179-184
3. Ma X, Wang Z, Liu F, Bian J (2010) A trust model based on the extended subjective logic for P2P networks. In: 2nd International conference on e-business and information system security. IEEE, Wuhan, China, pp 1-4
4. Kurdi, H., Alfaries, A., Al-Anazi, A. et al. A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. J Supercomput 75, 3534–3554 (2019). https://doi.org/10.1007/s11227-018-2669-y

5. Shvachko K, Kuang H, Radia S, Chansler R (2010) The hadoop distributed file system. In: 26th Symposium on mass storage systems and technologies (MSST). IEEE, Incline Village, NV, USA, pp 1-10
6. Rao S, Wang Y, Tao XL (2010) The comprehensive trust model in P2P based on improved eigentrust algorithm. In: International conference on measuring technology and mechatronics automation. IEEE, Changsha City, China, pp 822-825
7. Khan SM, Hamlen KW (2012) Hatman: intra-cloud trust management for hadoop. In: 5th International conference on cloud computing. IEEE, Honolulu, HI, USA, pp 494-501
8. Nishikawa T, Fujita S (2010) An effective risk avoidance scheme for the eigentrust reputation management system. In: 1st International conference on networking and computing. IEEE, Higashi-Hiroshima, Japan, pp 36-43
9. Abrams Z, Mcgrew R, Plotkin S (2005) A non-manipulable trust system based on EigenTrust. ACM SIGecom Exch 5:21-30
10. Jaiganesh M, Aarthi M, & Kumar AVA (2015) Fuzzy ART-Based User Behavior Trust in Cloud Computing. in Artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Eds.New Delhi: Springer:341-348.