УДК 681.03.06

К.А. ПОГРЕБНЯК, канд. техн. наук, Д.В. ПОВТАРЄВ

МОДЕЛЬ ВИКОРИСТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ ДЛЯ ЗАДАЧ АСИМЕТРИЧНОГО КРИПТОАНАЛІЗУ НА ПРИКЛАДІ ФАКТОРИЗАЦІЇ ЧИСЕЛ МЕТОДОМ ρ-ПОЛЛАРДА

Вступ

Інформаційні технології традиційно є галуззю знань, в якій нові підходи розвиваються напрочуд швидко. Сьогодні одним з таких підходів є впровадження технології хмарних обчислень. Наразі створюється велика кількість нових хмарних сервісів, проходить етап міграції існуючих веб додатків до хмар, а також виходять публікації на тему використання хмарних рішень для все більшого класу задач. Все це свідчить про не аби яке зацікавлення технологією світовою спільнотою, зокрема провідними корпораціями та науковим співтовариством [1].

По-суті, хмарні обчислення є динамічно масштабованим способом доступу до зовнішніх обчислювальних ресурсів у вигляді сервісу, що надається за допомогою Інтернету, при цьому користувачам не потрібні особливі знання про інфраструктуру хмари або навички управління цією технологією. Фактично, використовуючи різні рівні хмарних обчислень, користувач буде отримувати доступ до деякого програмного забезпечення (рівень *SaaS – Software as a Service*), інтегрованої платформи (рівень *PaaS – Platform as a Service*) чи навіть комп'ютерної інфраструктури (рівень *IaaS – Infrastructure as a Service*), які будуть надаватися на вимогу як сервіси [2].

Слід відзначити, що на даному етапі потенціал хмарних обчислень не враховується в повному обсязі відносно їх впливу на інші технології, зокрема у галузі використання асиметричної криптографії.

За останні десятиріччя асиметрична криптографія поширилась на усі сфери життя сучасної людини. Її використання для економічних, політичних, військових задач визначається вимогою дотримання найвищого рівня безпеки, що ґрунтується на стійкості криптографічних примітивів. Оцінка стійкості криптографічних примітивів традиційно базується на виборі найбільш ефективного методу криптоаналізу та подальшому отриманні емпіричних характеристик обраного методу. Критерієм ефективності методу, як правило, вважається мінімізація обчислювальних ресурсів, тобто просторово часових показників. В той же час оцінки методів криптоаналізу у повному обсязі не враховують використання хмарних обчислень.

Таким чином, актуальною задачею є розробка моделі використання обчислювальних ресурсів у хмарі для різних методів криптоаналізу.

1. Модель використання хмарних обчислень для задач криптоаналізу

Застосування технології хмарних обчислень для задач криптоаналізу має ряд суттєвих переваг і, водночас, не позбавлено певних недоліків. Сукупність таких переваг та недоліків визначає вимоги до моделі використання хмарних обчислень у задачах криптоаналізу. Розглянемо більш детально переваги та недоліки використання хмарних обчислень та сформуємо основні вимоги до криптоаналітичної моделі.

1.1. Переваги та недоліки використання хмарних обчислень у задачах криптоналізу

Серед переваг технології хмарних обчислень, що мають суттєве значення для задач криптоаналізу, слід в першу чергу виділити наступні [3, 4]:

• Динамічна масштабованість системи. Обчислювальна потужність, яка доступна користувачу хмарних систем, практично обмежена лише розміром хмари, тобто загальною кількістю віддалених серверів. Користувачі можуть виконувати більш складні задачі, що потребу-

ють потужні процесори, велику кількість пам'яті та місце для зберігання даних, а система сама буде виділяти на це ресурси оптимальним чином та у необхідному обсязі.

• Спрощення адміністрування системи. Програмне забезпечення, що розгорнуто в хмарі, є захищеним та завжди підтримується в актуальному стані відповідними механізмами технології хмарних обчислень.

• Незалежність функціонування системи від пристроїв доступу до неї. Користувачі криптоаналітичної системи, побудованої на концепції хмарних обчислень, мають можливість доступу до неї фактично з будь-якого пристрою, який є підключеним до мережі Інтернет.

• Стійкість до непередбачених збоїв та фізична захищеність. Особливості функціонування хмарних систем забезпечують надійне виконання поставлених задач з низькою мірою залежності від стану певного апаратного вузла на якому виконуються обчислення.

Серед недоліків використання технології хмарних обчислень для задач криптоаналізу слід виділити наступні:

• Зберігання та контроль інформації за межами організації. Інформація, що зберігається за межами організації потенційно, може бути розкрита власниками системи хмарних обчислень, в якій вона циркулює. Власник криптоаналітичної системи не може в повному обсязі контролювати інформацію, що знаходиться в хмарі.

• Відсутність типових рішень та стандартів у зв'язку з новизною технології. Стандарти та технічні вимоги, що регулюють базові аспекти побудови хмарних систем та можуть в певному обсязі гарантувати безпеку інформації, знаходяться на етапі формування.

• Через особливості архітектури втрата даних в хмарі є безоборотною.

• Особливості створення програмних продуктів для розгортання у хмарах на різних платформах та, як наслідок, відповідні обмеження на міграцію від одного постачальника послуг до іншого.

1.2. Вимоги до моделі використання хмарних обчислень для задач криптоаналізу

Виходячи з переваг і недоліків технології хмарних обчислень можна висунути наступні вимоги до криптоаналітичної системи:

• Архітектура криптоаналітичної системи повинна бути багатомодульною. Модуль керування повинен бути відокремленим та знаходитись на комп'ютері, яким володіє користувач.

• Необхідність забезпечення моніторингу роботи криптоаналітичної системи та резервне копіювання цінної інформації.

• Незалежність криптоаналітичної системи від вибору платформи та забезпечення її функціонування при переході до будь-якого постачальника сервісу хмарних обчислень.

• Так як однією з найсуттєвіших причин використання хмарних технологій для задач криптоаналізу є низька вартість обчислювальних потужностей, то необхідно обирати найбільш економічно доцільний сервіс. Обчислювальні потужності повинні бути суттєво дешевшими ніж при створенні аналогічною за потужністю системи.

1.3. Опис моделі використання хмарних обчислень для задач криптоаналізу

Виходячи зі сформованих вимог, загальні компоненти криптоаналітичної системи, повинні включати:

- модуль керування криптоаналітичною системою;
- модуль моніторингу криптоаналітичної системи;
- модулі, що використовують обчислювальні ресурси:
  - на основі глобальної мережі Інтернет;
  - на основі локальної обчислювальної мережі;
  - на основі сервісу хмарних обчислень.

Графічне представлення загальних компонентів розподіленої криптоаналітичної системи наведено на рис. 1.

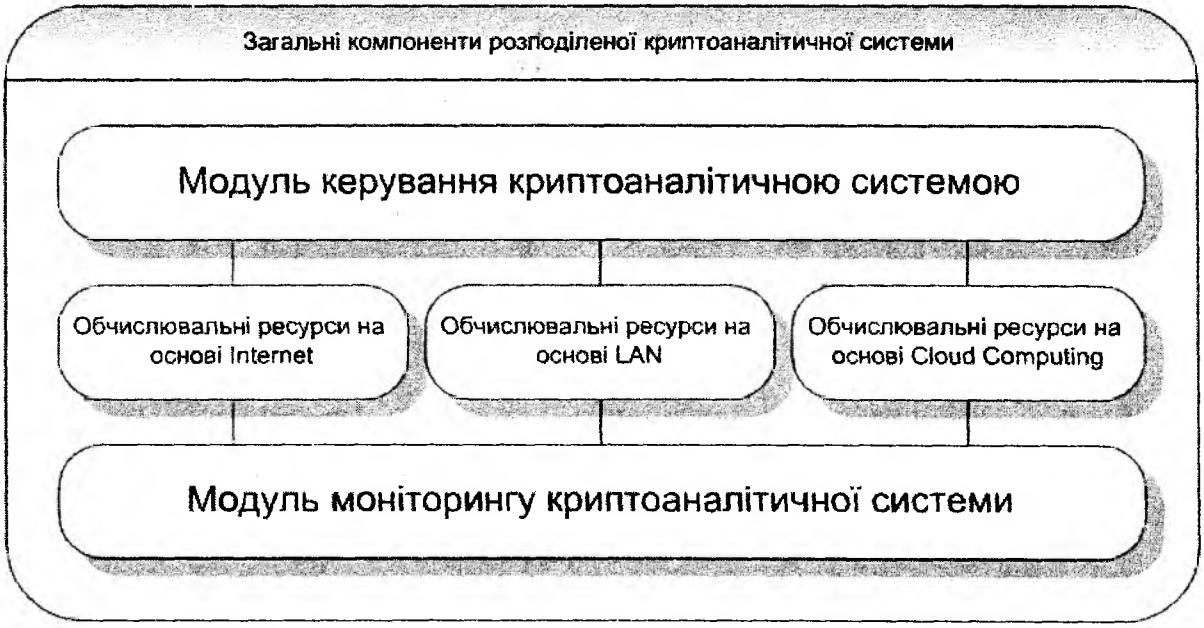

Рис.1

Для використання переваг технології хмарних обчислень та мінімізації ризиків, які пов'язані з нею, доцільним є одночасне використання модулів, що використовують усі обчислювальні ресурси.

Порівняння модулів, що використовують різні обчислювальні ресурси наведено в табл. 1.

Таблиця 1

Критерій порівняння	Обчислювальні ресурси на основі Internet	Обчислювальні ресурси на основі LAN	Обчислювальні ресурси на основі Cloud Computing
Стабільність роботи модуля системи	–	+	+
Контроль з боку власника системи	–	+	–
Наявність стабільного каналу передачі даних	+	–	+
Висока вартість володіння системою	–	+	–

Відмітимо, що основний модуль криптоаналітичної системи базується на використанні ресурсів локальної обчислювальної мережі. Такий модуль є найбільш надійним, оскільки він повністю контролюється власником системи, має фіксовану кількість робочих станцій, що гарантує певні показники потужності системи, та забезпечує контроль за резервним зберіганням інформації. Проте використання тільки ресурсів на основі локальної обчислювальної мережі є досить дорогим, так як вимагає коштів на створення та подальшу підтримку робочих станцій та серверів.

Модуль, що використовує обчислювальні ресурси у мережі Інтернет, є найменш стабільним та не забезпечує гарантійний рівень показників потужностей. З іншого боку такий компонент системи є абсолютно безкоштовним.

Модуль, що використовує ресурси на основі хмарних обчислень, є досить стабільним з гарантованим рівнем показників потужностей та зменшеною вартістю володіння системою в порівнянні з модулем, що ґрунтується на використанні ресурсів локальної обчислювальної

мережі. Недоліком такого компонента системи є неповний контроль з боку власника криптоаналітичної системи та наявність стабільного каналу передачі даних.

Використання різних обчислювальних ресурсів дозволяє визначати необхідний рівень потужності системи та вартість володіння нею.

2. Модель використання хмарних обчислень для задачі факторизації чисел методом ρ-Полларда

Безпека більшості сучасних криптосистем базується на складності задачі факторизації чисел.

Розглянемо побудування компонента системи, який використовує ресурси на основі хмарних обчислень, на прикладі розв'язання задачі факторизації чисел методом ρ-Полларда.

2.1. Опис методу ρ-Полларда факторизації чисел

Простота реалізації та відсутність залежності від структури групи зробили саме цей алгоритм найбільш прийнятним на цьому етапі досліджень. Метод ρ-Полларда базується на тому, що число N має такий простий дільник p, для якого $p-1$ є добутком невеликих простих чисел. Тому цей метод є ефективним при факторизації складених чисел з невеликими множниками у розкладенні.

Наведемо формальний опис алгоритму ρ-Полларда [5]:

Нехай N складене ціле додатне число.

Крок 1. Обираємо число k, що є добутком невеликих простих чисел в невеликих степенях. Наприклад, $k = НСК\{2,3,...M\}$ для деякого цілого додатного числа M.

Крок 2. Обираємо довільне число a, що задовольняє умові $1 < a < n$.

Крок 3. Обчислюємо найбільший спільний дільник $НСД(a,n)$. Якщо $НСД(a,n) > 1$ то ми отримуємо нетривіальний співмножник n. Якщо $НСД(a,n) = 1$, то переходимо до наступного кроку.

Крок 4. Обчислюємо $D = НСД(a^k - 1, n)$.

Якщо $1 < D < n$, то D є дільником числа N. Якщо $D = 1$, то повертаємося до кроку 1 та обираємо більший показник k. Якщо $D = n$ повертаємося до кроку 2 і обираємо нове число a.

2.2. Опис моделі використання хмарних обчислень для задачі факторизації чисел

Виходячи з наявної моделі та поставленої задачі побудуємо спрощену модель криптоаналітичної системи, яка буде використовувати ресурси тільки на основі хмарних обчислень.

Визначимо основні компоненти моделі:

- обчислювальний модуль криптоаналітичної системи;
- модуль керування криптоаналітичною системою;
- модуль моніторингу критоаналітичної системи;
- віддалений модуль керування криптоаналітичною системою;
- віддалений модуль моніторингу критоаналітичної системи.

Основними вимогами до спрощеної моделі є:

- наявність надійного канал Інтернет з'єднання;
- використання хмарного сервісу рівня PaaS;
- наявність засобу доступу до мережі Інтернет.

Графічний опис спрощеної моделі наведено на рис. 2.

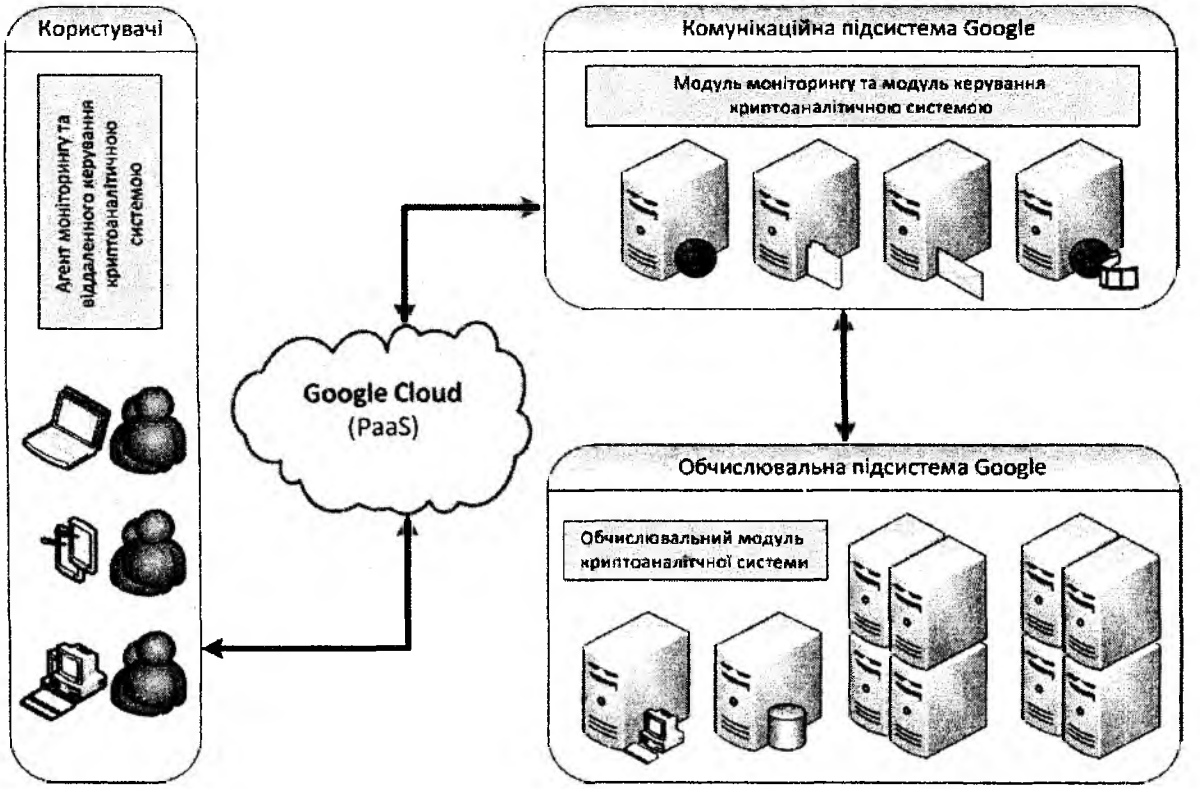

Рис.2

3. Реалізація моделі використання хмарних обчислень для задачі факторизації чисел методом ρ-Полларда з використанням технології Google App Engine

Для спрощення реалізації моделі використання хмарних обчислень для задачі факторизації чисел методом ρ-Полларда була обрана технологія Google App Engine (GAE), оскільки вона дозволяє розробляти, адмініструвати та масштабувати додатки, не зважаючи на апаратні засоби та резервне копіювання інформації. GAE надає доступ до інтегрованої платформи, тобто функціонує на рівні PaaS [6].

З застосуванням технології Google App Engine та мови програмування Java створено програмний продукт, що проводить факторизацію чисел за допомогою алгоритму ρ-Полларда на стороні сервера, тобто в хмарі Google [7].

Для підтвердження ефективності використання технологій хмарних обчислень для задач криптоаналізу проведене порівняння ефективності виконання факторизації за методом ρ-Полларда з використанням одного і того ж додатку, розгорнутому в хмарі та на персональному комп'ютері. Виконана факторизація чисел різної бітової довжини з різною кількістю співмножників.

Моделювання роботи програми проведено у такий спосіб. Проведено по 20 вимірювань для кожного довільно фіксованого складеного числа, мінімальні значення яких занесені до таблиці. Обчислення, що виконуються на стороні сервера, використовують потужності хмари і в кожен момент часу отримують необхідні ресурси, розмір яких контролює система. Проаналізувавши результати та порівнявши значення, можна зробити висновок, що зі збільшенням бітової довжини та кількості співмножників ефективність використання хмарних обчислень для задач криптоаналізу зростає.

Моделювання проводилось на комп'ютері з ОС – Microsoft Windows 7 Enterprise SP1 x86, процесором – Intel(R) Core (TM) 2 Duo 2,33 GHz, ROM – 3,50 Gb.

Результати виконання обчислень представлені у табл. 2.

Таблиця 2

№	Бітова довжина, *біт*	Кількість співмножників	Число/ Розклад числа	Час розкладу в хмарі, *мс*	Час розкладу на ПК, *мс*
1	74	5	**104353695894386059276 49** [313, 101, 745673, 254537, 1739173]	3	7
2	105	5	**353534543655432351365543457345 35** [5, 2803, 199, 1105774941389, 11463544797179]	4380	8845
3	105	19	**401553784227617377474369397350 40** [2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 7, 5, 23, 239, 123017, 11267303, 36762487387]	14	17
4	106	7	**493771156082948827115616533485 32** [2, 2, 3, 3, 3, 284927963, 1604600370135027022133]	182	192
5	106	13	**809873657435071567269852918946 20** [2, 2, 5, 11, 13, 101, 101, 107, 103, 211, 1739173, 745673, 907223]	3	16
6	107	13	**985287111111110898378666659948 80** [2, 2, 2, 2, 2, 2, 2, 5, 7, 47, 67, 35026304461, 199396627523279]	438	1867
7	107	19	**865123599856973844742274679582 72** [2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 3, 107, 101, 1879, 4027, 254537, 907223, 745673]	5	7
8	107	19	**946175999999999795711999993548 80** [2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 7, 5, 7, 3, 35026304461, 199396627523279]	1017	1490
9	113	5	**958745583769558766685874558769558 7** [3, 3, 317, 1739173, 193222999807667261092252 3]	4	22
10	124	2	**109545874558376955876668587455876955 87** [6777349, 16163528624300881639217426674 63]	10	32
11	137	5	**109548834587455837695587666858745587695587** [3, 7, 17041, 139091, 22008698503808543904256456446 37]	3	9
12	148	4	**235109548834887455837675587666859745587695587** [3, 3, 379, 689268686118110395302479002248196263816 17]	2	3
13	153	4	**107154823645985214654897542313456564213246547 97** [23, 1852579, 1216358616623, 20674999945252002116276896 7]	10710	14154
14	166	4	**555672341095488345874558376955876668587455876955 87** [71, 431, 907223, 2001562285545371538453585678573842585069]	12	14
15	172	3	**567556723410954883458745583869558766685874558769558 7** [3, 60611333, 3121290443658750987810291648865725967374641 3]	140	325
16	182	7	**456545788200019878978978978562139835455677647987954340** [2, 2, 5, 331, 4027, 197161, 868607768752751109739690292551110374498981]	7	7
17	182	7	**456545788200019878978978978562139835455677647987954340** [2, 2, 5, 331, 4027, 197161, 868607768752751109739690292551110374498981]	9	10
18	184	5	**156755672341095488345874567750837695586668587455876955 87** [13, 17, 46021, 745673, 206693358512674889579069789337680023648885 9]	8	15
19	186	5	**756755669341995488345874586775083769558666858745587695 58** [2, 7, 13, 254537, 163355354357039542718497366231711249207334061613 7]	10	20
20	187	6	**985655332155653535554897946205026776206634866660489066 0** [2, 2, 3, 5, 105051229, 156376931775442841884868983719124738912012710 59]	100	207

Висновки

Робота присвячена вирішенню задачі розробки моделі використання обчислювальних ресурсів у хмарі для різних методів криптоаналізу.

Проаналізовано переваги та недоліки використання хмарних обчислень у задачах криптоналізу, на основі яких сформовано перелік вимог до криптоаналітичної системи.

Розроблено загальну модель використання хмарних обчислень для задач асиметричного криптоаналізу. Загальні компоненти криптоаналітичної системи повинні включати одночасно модулі, які використовують обчислювальні ресурси на основі глобальної мережі Інтернет, на основі локальної обчислювальної мережі та на основі сервісу хмарних обчислень. Але основний модуль криптоаналітичної системи повинен базуватися на використанні ресурсів локальної обчислювальної мережі, оскільки є найбільш надійним.

Визначено, що модуль, який використовує ресурси на основі хмарних обчислень, є досить стабільним та характеризується зменшеною вартістю володіння системою в порівнянні з модулем, що ґрунтується на використанні ресурсів локальної обчислювальної мережі. Тобто використання ресурсів на основі хмарних обчислень дозволяє зменшити вартість володіння в обмін на неповний контроль з боку власника криптоаналітичної системи та наявність стабільного каналу передачі даних.

На основі загальної моделі розроблена часткова модель для розв'язання задачі факторизації чисел методом ρ-Полларда, яка використовує ресурси тільки на основі хмарних обчислень. Реалізація часткової моделі використовує технологію Google App Engine та мову програмування Java.

За результатами моделювання процесу розв'язання задачі факторизації чисел методом ρ-Полларда у хмарі можна зробити висновок, що зі збільшенням бітової довжини та кількості співмножників ефективність використання хмарних обчислень для задач криптоаналізу зростає.

У подальшому планується розширити кількість методів криптоаналізу, відокремити модуль керування та реалізувати віддалений агент моніторингу.

Сервіс, що реалізує розв'язання задачі факторизації чисел методом ρ-Полларда, є загальнодоступним та знаходиться за адресою http://factorintegers.appspot.com.

Список літератури: 1. *John W. Rittinghouse, James F. Ransome.* Cloud Computing: Implementation, Management, and Security. CRC Press, 2009. 340 p. 2. *Tim Mather, Subra Kumaraswamy, Shahed Latif.* Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, 2009. 334p. 3. *Toby Velte, Anthony Velte, Robert Elsenpeter.* Cloud Computing, A Practical Approach. McGraw Hill Professional, 2009. 352 p. 4. *Barrie Sosinsky.* Cloud Computing Bible. John Wiley & Sons, 2010. 672p. 5. *Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L. & Stein, Clifford.* Introduction to Algorithms (Second ed.). Cambridge, MA: MIT Press. 2001. 896–901pp. 6. *Sanderson, Dan.* Programming Google App Engine (1st ed.). O'Reilly Media. 2009. 400 p. 7. *Charles Severance.* Using Google App Engine. O'Reilly Media, Inc. 2009. 272 p.

Харківський національний університет радіоелектроніки

Надійшла до редколегії 23.09.2012