Tom 3, wydanie 3, marzec 2013 ISSN: 2277 128X

International Journal of Advanced Research w Informatyka i inżynieria oprogramowania

Artykuł badawczy

Dostępny w Internecie pod adresem: www.ijarcsse.com

Bezpieczeństwo przechowywania i przesyłania danych w Chmura obliczeniowa

Pradnyesh Bhisikar [#1],
#1M.E (uczony),
GHRaisoni College of Engineering and Management, Amravati.

Prof. Amit Sahu [*2]
*2M.E (CSE),
GHRaisoni College of Engineering and Management, Amravati.

Streszczenie — Cloud Computing został pomyślany jako architektura nowej generacji IT Enterprise. W chmurze dane przesyłane są pomiędzy serwerem a klientem. Wysoka prędkość jest ważną kwestią w sieci. Bezpieczeństwo w chmurze to aktualny temat dyskusji w świecie IT. Ten artykuł badawczy pomaga w zabezpieczeniu danych bez wpływu na warstwy sieci i ochronie danych przed nieupoważnionym wejściem na serwer. Dane są zabezpieczane na serwerze w oparciu o wybraną przez użytkownika metodę bezpieczeństwa, dzięki czemu dane mają wysoki priorytet bezpieczeństwa. Chmura obliczeniowa jest uważana za architekturę nowej generacji IT Enterprise. W przeciwieństwie do tradycyjnych rozwiązań, gdzie usługi IT znajdują się pod odpowiednią kontrolą fizyczną, logiczną i personalną, Cloud Computing przenosi oprogramowanie aplikacyjne i bazy danych do dużych centrów danych, gdzie zarządzanie danymi i usługami może nie być w pełni godne zaufania. Ta wyjątkowa cecha stwarza jednak wiele nowych wyzwań związanych z bezpieczeństwem, które nie zostały dobrze poznane. W tym artykule skupiamy się na bezpieczeństwie przechowywania i transmisji danych w chmurze, które od zawsze było ważnym aspektem jakości usług. Aby zapewnić poprawność danych użytkowników w chmurze, proponujemy efektywny i elastyczny schemat rozproszony z dwiema istotnymi cechami, w przeciwieństwie do swoich poprzedników. [1]Przechowywanie w chmurze umożliwia użytkownikom zdalne przechowywanie danych i korzystanie z wysokiej jakości aplikacji w chmurze na żądanie bez konieczności lokalnego zarządzania sprzętem i oprogramowaniem. W tym artykule omówiono bariery i rozwiązania utrudniające zapewnienie godnego zaufania środowiska przetwarzania w chmurze.

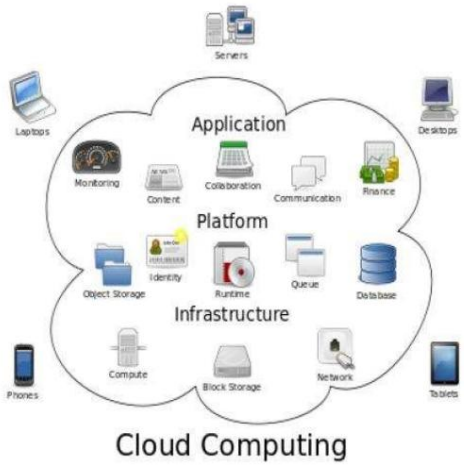
Słowa kluczowe – Chmura, Chmura prywatna, Bezpieczeństwo, Bezpieczna transmisja danych.

I. WSTĘP

Przetwarzanie w chmurze to najnowszy trend w IT, polegający na tym, że przetwarzanie i przechowywanie danych odbywa się w centrach danych, a nie na osobistych przenośnych komputerach PC. Dotyczy aplikacji dostarczanych jako usługi przez Internet, a także infrastruktury chmurowej – czyli sprzętu i oprogramowania systemowego w centrach danych świadczących tę usługę. Dzielenie się zasobami zmniejsza koszty dla poszczególnych osób. Najlepszą definicję chmury definiuje się w [9] jako dużą pulę łatwo dostępnych i zwirtualizowanych zasobów, które można dynamicznie rekonfigurować w celu dostosowania do zmiennego obciążenia, co pozwala również na optymalne wykorzystanie skali. Kilka trendów otwiera erę Cloud Computing, czyli rozwoju i wykorzystania technologii komputerowej w oparciu o Internet. Kluczowymi siłami napędowymi przetwarzania w chmurze jest wszechobecność sieci szerokopasmowych i bezprzewodowych, spadające koszty przechowywania danych oraz postępujące udoskonalenia oprogramowania komputerowego do Internetu. Główne wsparcie techniczne infrastruktury i usług przetwarzania w chmurze obejmuje wirtualizację, oprogramowanie zorientowane na usługi, technologie przetwarzania sieciowego, zarządzanie dużymi obiektami i efektywność energetyczną. Pionier dostawców usług przetwarzania w chmurze, Amazon Simple Storage Service (S3) i Amazon Elastic Compute Cloud (EC2) [1] to dobrze znane przykłady. Chociaż te internetowe usługi online rzeczywiście zapewniają ogromną ilość miejsca na dysku i konfigurowalne zasoby obliczeniowe, jednak ta zmiana platformy obliczeniowej eliminuje jednocześnie odpowiedzialność lokalnych maszyn za konserwację danych. W rezultacie użytkownicy są zdani na łaskę dostawców usług w chmurze, jeśli chodzi o dostępność i integralność ich danych. Przykładem może być niedawna awaria S3 firmy Amazon [2]. Z punktu widzenia bezpieczeństwa danych, które zawsze było ważnym aspektem jakości usług, przetwarzanie w chmurze nieuchronnie stwarza nowe, trudne zagrożenia bezpieczeństwa z wielu powodów. Po pierwsze, tradycyjnych prymitywów kryptograficznych do celów ochrony bezpieczeństwa danych nie można bezpośrednio zastosować ze względu na utratę przez użytkowników kontroli nad danymi w ramach Cloud Computing. Biorąc pod uwagę różne rodzaje danych każdego użytkownika przechowywanych w chmurze oraz potrzebę długoterminowego, ciągłego zapewnienia bezpieczeństwa jego danych, problem weryfikacji prawidłowości przechowywania danych w chmurze staje się jeszcze większym wyzwaniem. Po drugie, Cloud Computing to nie tylko hurtownia danych stron trzecich. Dane przechowywane w chmurze mogą być często aktualizowane przez użytkowników, włączając w to wstawianie, usuwanie, modyfikowanie, dołączanie, zmianę kolejności itp. Taka konstrukcja drastycznie zmniejsza obciążenie związane z komunikacją i przechowywaniem w porównaniu z tradycyjnymi technikami dystrybucji plików opartymi na replikacji. Prace nad tym dokumentem są jedną z pierwszych w tej dziedzinie, które rozważają rozproszone przechowywanie danych w chmurze obliczeniowej. Po drugie, bezpieczna transmisja danych. Kluczowymi cechami chmury są elastyczność, koszt, niezależność od urządzeń i lokalizacji, wielodostępność, niezawodność, skalowalność, konserwacja itp. Poniższ

Pozostała część artykułu jest zorganizowana w następujący sposób. Część II przedstawia model systemu, część III przedstawia model przeciwnika, część IV przedstawia nasz cel projektowy. W dziale V architektura bezpieczeństwa. Następnie zapewniamy bezpieczeństwo

sieci serwer-klient w dziale VI. Następnie podajemy szczegółowy projekt systemu oraz szczegółowo o transmisji danych w Rozdziale VII. Wreszcie w Rozdziale VIII zawarto uwagę końcową całego artykułu.



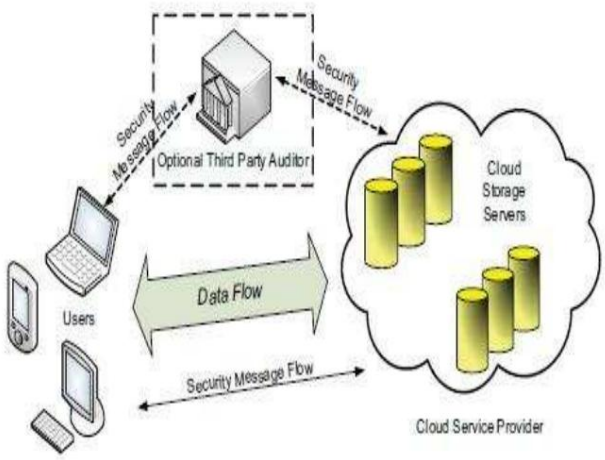
Rysunek 1 – ogólna struktura przetwarzania grudkowego

II. Model systemu W

[1] i [2] Reprezentatywną architekturę sieci do przechowywania danych w chmurze przedstawiono na rysunku 2. Można zidentyfikować trzy różne jednostki sieciowe w następujący sposób:

- Użytkownik: użytkownicy, którzy przechowują dane w chmurze i polegają na chmurze do obliczania danych, to zarówno indywidualni konsumenci, jak i organizacje.
- Dostawca usług w chmurze (CSP): CSP, który posiada znaczne zasoby i wiedzę specjalistyczną w zakresie budowania rozproszonych serwerów pamięci masowej w chmurze i zarządzania nimi, jest właścicielem i operatorem działających systemów Cloud Computing.
- Audytor strony trzeciej (TPA): opcjonalny TPA, posiadający wiedzę i możliwości, których użytkownicy mogą nie mieć, może na żądanie ocenić i ujawnić ryzyko związane z usługami przechowywania w chmurze w imieniu użytkowników.

W przypadku przechowywania danych w chmurze użytkownik przechowuje swoje dane za pośrednictwem dostawcy CSP na zestawie serwerów w chmurze, które działają jednocześnie, współpracują i rozproszone. Można zastosować nadmiarowość danych wraz z techniką korygowania usuwania danych, aby lepiej tolerować błędy lub awarie serwera w miarę wzrostu rozmiaru i znaczenia danych użytkownika . Następnie, na potrzeby aplikacji, użytkownik wchodzi w interakcję z serwerami w chmurze za pośrednictwem CSP, aby uzyskać dostęp do swoich danych lub je odzyskać. W niektórych przypadkach użytkownik może być zmuszony do wykonania operacji na poziomie bloków na swoich danych. Najbardziej ogólne formy tych operacji, które rozważamy, to aktualizacja blokowa, usuwanie, wstawianie i dołączanie. W naszym modelu zakładamy, że kanały komunikacji punkt-punkt pomiędzy każdym serwerem w chmurze a użytkownikiem są uwierzytelnione i niezawodne, co w praktyce można osiągnąć przy niewielkim nakładzie finansowym. Należy pamiętać, że w tym dokumencie nie poruszamy kwestii prywatności danych, ponieważ w przypadku przetwarzania w chmurze prywatność i przechowywanie danych są ortogonalne w stosunku do badanego tutaj problemu.



Rysunek 2 – architektura przechowywania danych w chmurze.

III. Model przeciwstawny

Zagrożenia bezpieczeństwa, na które narażone są przechowywanie danych w chmurze, mogą pochodzić z dwóch różnych źródeł. Z jednej strony dostawca usług internetowych może kierować się własnym interesem, nie można mu ufać i być może jest złośliwy. Nie tylko chce przenieść dane, które nie były lub są rzadko dostępne na niższy poziom pamięci masowej niż uzgodniono ze względów finansowych, ale może również próbować ukryć przypadek utraty danych z powodu błędów w zarządzaniu, zawiłych awarii i tak dalej. Z drugiej strony może istnieć również przeciwnik motywowany ekonomicznie, który może złamać zabezpieczenia wielu serwerów przechowywania danych w chmurze w różnych odstępach czasu i

może następnie modyfikować lub usuwać dane użytkowników, pozostając przez pewien czas niewykrytym przez dostawców usług internetowych.
W tym artykule rozważymy w szczególności dwa typy przeciwników o różnych poziomach możliwości: Słaby przeciwnik: Przeciwnik jest zainteresowany uszkodzeniem plików danych użytkownika przechowywanych na poszczególnych serwerach. Po utworzeniu serwera przeciwnik może zanieczyścić oryginalne pliki danych, modyfikując lub wprowadzając własne fałszywe dane, aby uniemożliwić użytkownikowi odzyskanie oryginalnych danych. Silny przeciwnik: Jest to najgorszy scenariusz, w którym zakładamy, że przeciwnik może skompromitować wszystkie serwery pamięci masowej, aby móc celowo modyfikować pliki danych, o ile są one wewnętrznie spójne. W rzeczywistości jest to równoznaczne z przypadkiem, w którym wszystkie serwery współdziałają, aby ukryć incydent utraty lub uszkodzenia danych.

IV. Cele projektu

Aby zapewnić bezpieczeństwo i niezawodność przechowywania danych w chmurze w ramach wyżej wymienionego modelu przeciwnego, naszym celem jest zaprojektowanie skutecznych mechanizmów dynamicznej weryfikacji i działania danych oraz osiągnięcie następujących celów: (1)
Poprawność przechowywania: zapewnienie użytkownikom, że ich dane są faktycznie przechowywane prawidłowo i cały czas przechowywany w nienaruszonym stanie w chmurze.

(2) Szybka lokalizacja błędu danych: aby skutecznie zlokalizować nieprawidłowo działający serwer w przypadku wykrycia uszkodzenia danych.
(3) Dynamiczna obsługa danych: aby utrzymać ten sam poziom zapewnienia poprawności przechowywania, nawet jeśli użytkownicy modyfikują, usuwają lub dołączają swoje pliki danych w chmurze.
(4) Niezawodność: w celu zwiększenia dostępności danych przed awariami bizantyjskimi, złośliwymi modyfikacjami danych i atakami w ramach zmowy serwerów, tj. minimalizowanie skutków błędów w danych lub awarii serwerów.
(5) Lekki: umożliwia użytkownikom sprawdzanie poprawności przechowywania przy minimalnym nakładzie pracy.

V. Architektury bezpieczeństwa

Powyższa dyskusja dotyczy pewnej literatury przeglądowej wielu badaczy na temat różnych aspektów bezpieczeństwa. Następnie opisano problemy i zagrożenia związane z bezpieczeństwem w chmurze. Literatura szczegółowo wyjaśnia takie kwestie, jak bezpieczeństwo danych, bezpieczeństwo wirtualizacji i zalecany format umowy SLA itp. Istnieje wielu badaczy żywo zainteresowanych projektowaniem określonych architektur bezpieczeństwa pomagających w bezpiecznym przetwarzaniu w chmurze. Poniżej opisano, co następuje: Gary Anthes [14] opisał różne prace badawcze dotyczące bezpieczeństwa w chmurze. Przywoływał prace badawcze prowadzone w popularnych firmach, takich jak IBM, HP i Microsoft. Istnieje wiele zagrożeń bezpieczeństwa związanych z przetwarzaniem w chmurze, a także badacze opracowali kilka dobrych rozwiązań, które wskazano poniżej. 1)

Naukowcy z laboratoriów HP prototypują komórki jako usługę automatyzującą zarządzanie bezpieczeństwem w chmurze. Komórka to pojedyncza domena administracyjna korzystająca z zasad bezpieczeństwa zawierających maszyny wirtualne, woluminy pamięci na maszynach fizycznych.
Pracownicy IBM

2) przeprowadzają introspekcję maszyn wirtualnych, która zapewnia bezpieczeństwo chronionej maszynie wirtualnej działającej na tej samej maszynie. Wykorzystuje to szereg metod ochronnych wymieniających funkcje jądra. Może zmniejszyć liczbę uruchomionych skanerów antywirusowych w systemie.

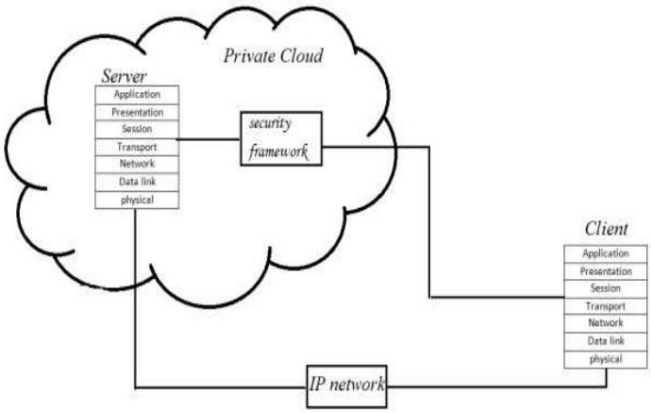
3) Badania Microsoftu opisywały przechowywanie w chmurze kryptograficznej, w której dane są zabezpieczane przez użytkownika poprzez szyfrowanie w taki sposób, że dostawca nie może uzyskać informacji o zawartości danych.

Flavio Lombardi i Roberto Di Pietro omawiali [15] bezpieczną technikę wirtualizacji zapewniającą bezpieczeństwo na poziomie hiperwizora. W ogólnym systemie na podstawowym poziomie systemu operacyjnego występuje problem polegający na tym, że użytkownik jednego systemu gościa może wchodzić w interakcję z innym systemem operacyjnym gościa, co może prowadzić do utraty danych w przypadku ataku. Wprowadzono więc nową propozycję ACPS (Advanced Cloud Protection System). Zapewni to bezpieczeństwo, zapobiegając niepotrzebnemu logowaniu się do innego systemu gościa przy użyciu słabych haseł lub słabego protokołu SSH. Cong Wang [5] zaproponował swoją pracę nad bezpieczeństwem przechowywania danych w odniesieniu do jakości usług. Zaproponowali podejście, które sprawdza, czy ich dane zostały zaatakowane lub czy nie doszło do utraty integralności w chmurze. Wygenerują token homomorfizmu, który zagwarantuje, że dane nie zostaną utracone. Przypomina to prostą funkcję skrótu, która umożliwia szybkie odzyskiwanie i przechowywanie błędów. Prace te pomagają w zabezpieczeniu systemów chmurowych, wirtualizacji, poufności danych i bezpieczeństwie przechowywania danych, nadal pozostają do omówienia kwestie związane z bezpieczną transmisją danych pomiędzy Dostawcą chmury, dostawcą usług i Użytkownikiem chmury. Bezpieczną transmisję danych w każdym razie zapewniają protokoły takie jak IPSec, SSL w Internecie, a dane przesyłane są również za pośrednictwem aplikacji internetowych. Obecne metody można wykorzystać do bezpiecznej transmisji danych. Prace nad bezpieczną transmisją danych przeznaczone dla sieci pamięci masowej omówił Kikuko Kamiasaka [8], który w swoim artykule omówił bezpieczną transmisję danych w sieciach IP poprzez opracowanie oprogramowania pośredniczącego działającego poniżej warstwy aplikacji i wybierającego odpowiednie podejście do bezpieczeństwa w oparciu o klaster elementów danych dostępnych w Aplikacja.
Udowodniono, że pomoże to w zabezpieczeniu danych i działa lepiej niż IPSec. Sudha M [3] zaproponował pomysł bezpiecznej transmisji danych w chmurze obliczeniowej z wykorzystaniem technik warstwy transportowej, w którym zaproponowano koncepcję programowania gniazd w celu bezpiecznej transmisji danych przez klienta i serwer. W artykule porównano ogólną bezpieczną transmisję danych poprzez zastosowanie programowania gniazd, wymiany kluczy i bezpiecznych danych w chmurze. Porównaniu podlega czas odpowiedzi i czas przetwarzania.

VI. Ramy bezpieczeństwa sieci serwer-klient

Ryc. 3 przedstawia architekturę projektu, w której zaprojektowano nową warstwę zabezpieczeń dla chmury prywatnej. Nowa struktura bezpieczeństwa znajduje się pomiędzy warstwą sesji a warstwą transportową, dzięki czemu jest przezroczysta dla warstwy aplikacji i niższych warstw. Zatem ilekroć klient przesyła dane, są one najpierw zabezpieczane przez określone protokoły uwierzytelniania i zapisywane po stronie serwera. Dzięki temu dane będą przechowywane w bezpieczny sposób na końcu serwera. Ci, którzy chcą pobrać

dane lub widok powinny być połączone lub mieć dostęp poprzez ten sam framework, aby przeglądać dane. Odbywa się to na poziomie użytkownika aplikacji, dzięki czemu dane zostaną zabezpieczone i przesłane tam, gdzie zachodzi potrzeba zakłócenia niższych warstw sieci.

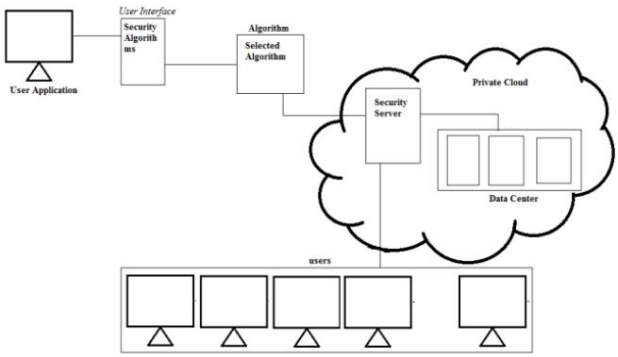


Rysunek 3 – projekt wysokiego poziomu

VII. PROJEKTOWANIE SYSTEMU

• Model ramowy bezpieczeństwa

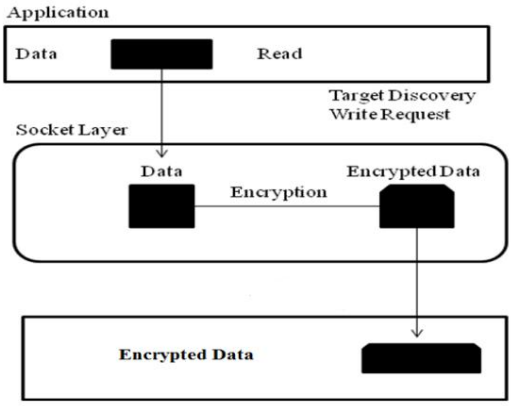
Szczegółowy projekt frameworku przedstawiono na poniższym rysunku architektury 4. Węzły podłączone do serwera zostaną połączone z warstwą bezpieczeństwa. Gdy użytkownik Aplikacji chce wysłać dane do chmury prywatnej, musi wybrać opcję



Rysunek 4 – architektura systemu

Algorytm bezpieczeństwa oparty na poziomie prywatności dokumentu, jeśli potrzebne jest większe bezpieczeństwo, należy wybrać silny algorytm bezpieczeństwa. Serwer bezpieczeństwa zabezpieczy dokument i zapisze go w bazie danych. Tutaj wszystkie systemy należące do tej sieci są podłączone do tej samej architektury. Jeśli inny użytkownik chce wybrać dowolny dokument z centrum danych, musi połączyć się z tym samym serwerem bezpieczeństwa, aby uzyskać oryginalny dokument. Pomaga to w bezpieczeństwie i prywatności dokumentów.

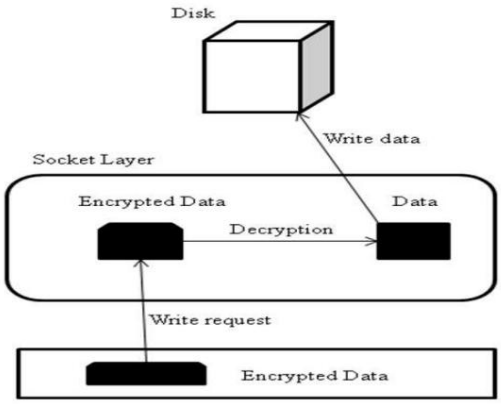
• Proces u nadawcy



Rysunek 5: proces u nadawcy

Wszystkie dane po stronie inicjatora (klienta) ustawią jego dane. Szyfruje dane wybierając odpowiednie podejście z interfejsu i wysyła je na koniec serwera. Jak pokazano na powyższym rysunku, po stronie klienta dane są odczytywane i gotowe do wysłania. W warstwie gniazda przed wysłaniem ich do zdalnego końca dane zostaną zaszyfrowane dla każdego bajtu i wysłane zaszyfrowane dane. Dane są przesyłane przez protokół w celu przetwarzania innych poleceń, które zachodzą w sieci. Dane będą zabezpieczone po stronie nadawcy za pomocą struktury bezpieczeństwa, która pomaga w bezpiecznym przesyłaniu danych.

• Proces po stronie odbiorcy



Rys. 6: proces w odbiorniku

Po odebraniu danych po stronie odbiorcy zostaną one odszyfrowane i zapisane na dysku. Dane zostaną odszyfrowane przy użyciu podejścia bezpieczeństwa zastosowanego na końcu szyfrowania. Jest to ponownie wykonywane powyżej warstwy transportowej, dokładnie tam, gdzie pakiety docierają do aplikacji końcowej. Podobnie jak wcześniej żądanie zapisu było wysyłane przez protokoły, struktura bezpieczeństwa odszyfrowuje dane i zapisuje je na dysku. W podobny sposób, gdy klient zażąda pliku z serwera, nastąpi ten sam proces, o którym mowa. Dzięki temu dane będą bezpieczne w sieci. Możemy przeprowadzić kontrolę poufności i integralności po stronie odbiorcy.

VIII. Wniosek

W artykule zbadaliśmy problem bezpieczeństwa danych przechowywanych i przesyłanych w chmurze, która jest zasadniczo rozproszonym systemem przechowywania. Aby zapewnić poprawność danych użytkowników w przechowywaniu danych w chmurze, zaproponowaliśmy efektywny i elastyczny schemat rozproszony. w naszym schemacie osiągamy integrację ubezpieczenia poprawności przechowywania i lokalizacji błędów danych. W proponowanej metodzie transmisji danych przesyłane dane są szyfrowane w wyższej warstwie, na górze warstwy transportowej, zamiast korzystać z protokołu IPSec lub SSL. W ten sposób można zastosować schemat poprawy wydajności bez modyfikowania implementacji warstwy IP i realizowana jest wydajna, bezpieczna komunikacja poprzez wstępne przetwarzanie szyfrowania w warstwie wyższej. Wykorzystaliśmy przesyłanie plików jako usługę jako aplikację internetową, bezpieczeństwo jest stosowane do danych w tle przy użyciu algorytmów szyfrowania, takich jak AES, Triple DES i DES. Dzięki szczegółowej analizie bezpieczeństwa i wydajności pokazujemy, że nasz system jest wysoce wydajny i odporny na awarie bizantyjskie, złośliwe ataki polegające na modyfikacji danych, a nawet ataki polegające na zmowie serwerów. Wierzymy, że bezpieczeństwo przechowywania danych w Cloud Computing, obszarze pełnym wyzwań i niezwykle ważnym, jest wciąż w powijakach, a wiele problemów badawczych nie zostało jeszcze zidentyfikowanych. Dodanie bezpiecznego przechowywania w chmurze przy użyciu proponowanego rozwiązania kryptograficznego oraz techniki szyfrowania plików z możliwością przeszukiwania będzie stanowić lepsze podejście do użytkownika w celu zapewnienia bezpieczeństwa danych. Zabezpieczenia w chmurze wykorzystujące kryptografię są już stosowane do bezpiecznego przechowywania danych, które można ulepszyć w celu zapewnienia bezpiecznej transmisji i przechowywania danych. Ciekawym pytaniem w tym modelu jest to, czy możemy skonstruować schemat zapewniający zarówno publiczną weryfikację, jak i zapewnienie poprawności przechowywania danych dynamicznych. Poza tym, wraz z badaniami nad dynamicznym przechowywaniem danych w chmurze, planujemy również zbadać problem precyzyjnej lokalizacji błędów danych.

Literatura

[1] Cong Wang, Qian WangKui Ren, Ning Cao i Wenjing Lou „W stronę bezpiecznych i niezawodnych usług pamięci masowej w chmurze obliczeniowej” Transakcje IEEE dotyczące usług obliczeniowych, tom. 5, nie. 2 kwietnia-czerwca 2012
[2] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou Jin Li „Włączanie publicznej kontroli i dynamiki danych dla bezpieczeństwa przechowywania w chmurze” Transakcje IEEE w systemach równoległych i rozproszonych, tom. 22, nie. 5 maja 2011 r. [3] Boris Tomas1 i Bojan Vuksic2 „Peer to Peer Distributed Storage and Computing Cloud System” Międzynarodowa konferencja na temat interfejsów technologii informatycznych, 25-28 czerwca 2012 r., cavtat, chorwacja [4] „Wyzwania dotyczące bezpieczeństwa i prywatności w przetwarzaniu w chmurze Environments” , którego współautorem jest IEEE Computer and Reliability, tj. listopad/grudzień 2010 [5] Subashini S, Kavitha V., „A Survey on Security Issues in Service Delivery Models of Cloud Computing”, Journal of Network and Computer Applications (2011) tom. 34 Numer 1, styczeń 2011 s. 1-11.
[6] Balachander RK, Ramakrishna P, A. Rakshit, „Zagadnienia bezpieczeństwa chmury, Międzynarodowa konferencja IEEE na temat usług obliczeniowych (2010),” s. 517-520.

Bhisihar i in., International Journal of Advanced Research in Computer Science and Software Engineering 3(3),
Marzec - 2013, s. 1-6 [7]
Kresimir Popovic, Željko Hocenski, „Zagadnienia i wyzwania związane z bezpieczeństwem przetwarzania w chmurze”, MIPRO 2010, s. 344-349.
[8] Amazon.com, „Amazon Web Services (AWS),” Online pod adresem http://aws. Amazon.com, 2008.
[9] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, „A Break in Clouds: Towards a Cloud Definition”, ACM SIGCOMM Computer Communication Review, tom. 39, nr 1, styczeń 2009, s. 50-55.
[10] Patrick McDaniel, Sean W. Smith, „Perspektywy: pochmurno z szansą na wyzwania i ulepszenia bezpieczeństwa”, IEEE Towarzystwa komputerowe i niezawodność (2010), s. 77-80.
[11] Sameera Abdulrahman Almulla, Chan Yeob Yeun, „Zarządzanie bezpieczeństwem przetwarzania w chmurze”, Zarządzanie systemami inżynieryjnymi i jego zastosowania (2010), s. 1-7.
[12] Steve Mansfield-Devine, „Niebezpieczeństwo w chmurach”, Bezpieczeństwo sieci (2008), 12, s. 9-11.
[13] Anthony T. Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing: podejście praktyczne, Tata Mc GrawHill 2010.

[14] Gary Anthes, „Bezpieczeństwo w chmurze”, w: ACM Communications (2010), tom 53, wydanie 11, s. 16–18.
[15] Lombardi F, Di Pietro R. Bezpieczna wirtualizacja w chmurze obliczeniowej. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.