Rozwiązania bezpieczeństwa oparte na blockchain dla systemów IoT

Kwestie bezpieczeństwa IoT mają wiele wspólnych cech z ogólnym bezpieczeństwem IT. Jednak w przypadku systemów IoT wymagana jest znacznie większa czułość i poufność, gdy systemy te wchodzą i cyfryzują prywatne życie osób. Niektóre ze zidentyfikowanych kluczowych problemów związanych z prywatnością w przypadku Internetu Rzeczy związanych z gromadzeniem danych osób fizycznych to nieautoryzowany nadzór, niekontrolowane generowanie i wykorzystywanie danych, nieodpowiednie uwierzytelnianie i zagrożenia bezpieczeństwa informacji . Wrażliwość technologii IoT wynika z wymagań bezpieczeństwa, takich jak poufność, integralność, autentyczność, prywatność, dostępność i regulacje. Bezpieczeństwo IoT ma problemy fizyczne i logiczne. Kwestie fizyczne pociągają za sobą ograniczone możliwości urządzeń IoT pod względem mocy obliczeniowej i pamięci, a zwykle także pod względem energii, ponieważ większość urządzeń IoT jest zasilana bateryjnie. Logiczne kwestie obejmują uwierzytelnianie, prywatność, ochronę przed złośliwym oprogramowaniem, standaryzację polityk i monitorowanie . Wdrożenie IoT rodzi wiele problemów bezpieczeństwa związanych z charakterystyką urządzeń IoT, takich jak potrzeba lekkich algorytmów kryptograficznych pod względem możliwości przetwarzania i pamięci oraz stosowanie standardowych protokołów, takich jak konieczność minimalizacji rozmiaru danych wymienianych między węzłami . Urządzenia IoT są bardziej podatne na zagrożenia bezpieczeństwa niż komputery połączone z Internetem, ze względu na ograniczone możliwości przetwarzania i zasoby pamięci pogarszające wdrażanie ochrony. Obecne przejście internetowego protokołu sieciowego z IPv4 na IPv6 oznacza, że coraz większa liczba urządzeń IoT posiada globalne adresy IP, co ułatwia identyfikację tych urządzeń jako celów ataków bezpieczeństwa. Ataki na bezpieczeństwo ułatwia również autonomiczne działanie i komunikacja urządzeń IoT. W związku z tym istnieje pilna potrzeba nowych i solidniejszych rozwiązań bezpieczeństwa dla systemów IoT. Internet i jego stos technologiczny są rozwijane od około czterech dekad. W tym czasie scentralizowana architektura klient-serwer miała fundamentalne znaczenie w budowaniu obecnych platform i usług. Z punktu widzenia IoT może to być również kłopotliwe, na przykład, gdy niezliczona liczba czujników bezprzewodowych musi przesłać swoje dane z powrotem do scentralizowanej usługi lub gdy usługa monolityczna powinna być w stanie dystrybuować aktualizacje zabezpieczeń do zdecentralizowanej lub rozproszonej sieci czujników . Te sieci czujników często skorzystałyby na zdecentralizowanej architekturze komunikacyjnej, która byłaby w dużym stopniu samorządna. Jedną z kwestii, która tradycyjnie stanowi przeszkodę w tworzeniu zdecentralizowanej architektury, jest zaufanie innych aktorów. Wprowadzenie kryptowaluty Bitcoin zakładało, że nie jest potrzebne zaufanie między dwiema stronami. Udało się to osiągnąć dzięki zintegrowaniu mechanizmu rozproszonego konsensusu jako dowodu walidacji nowych transakcji przy jednoczesnym przestrzeganiu wcześniejszej historii transakcji. Zostało to w konsekwencji rozszerzone na projektowanie uogólnionych transakcji poza sferą kryptowalut. Dziś ten uogólniony mechanizm często występuje pod nazwą technologii blockchain lub zdecentralizowanej księgi. Tu omówiono rozwiązania bezpieczeństwa oparte na blockchain dla IoT i zapewniono wgląd w aktualne trendy badawcze. Pokrótce omówiono technologię Blockchain oraz przedstawiono jej zastosowanie w środowiskach IoT. Dodatkowo opisano niektóre obecne wysiłki, aby technologia blockchain była odpowiednia dla IoT.

Wymogi regulacyjne

Niedawne zainteresowanie regulatora, szczególnie w UE, skłoniło do większego skupienia się na bezpieczeństwie i prywatności w sektorze IoT. Przyjęcie technologii blockchain jako realnego rozwiązania dla przyszłych systemów IoT w spełnianiu wymagań regulacyjnych oferuje ogromny potencjał. Jeśli chodzi o wymagania regulacyjne dotyczące projektowania urządzeń IoT, nowe dyrektywy i rozporządzenia zostały niedawno przyjęte przez Parlament Europejski. Wymogi te można uznać za jedne z najbardziej rygorystycznych na świecie i mają zastosowanie do producentów urządzeń

oraz dostawców usług i platform w dowolnym miejscu, jeśli dostarczają do Unii Europejskiej i/lub przetwarzają dane osobowe mieszkańców UE. Ponadto państwa członkowskie UE zapewniają również pewne regulacje sektorowe dotyczące obszarów przetwarzania poufnych informacji, takich jak opieka zdrowotna i usługi finansowe. W Stanach Zjednoczonych brakuje ogólnego prawa o ochronie danych lub prywatności, a zamiast tego opiera się głównie na raczej minimalnym ustawodawstwie sektorowym dotyczącym prywatności. Podejście Stanów Zjednoczonych utrudnia wyciągnięcie wspólnych wniosków dotyczących utrzymania określonego poziomu prywatności podczas projektowania systemów informatycznych. Na przykład, chociaż ten sam system IoT może być używany w różnych obszarach, brak wspólnego wymogu prywatności lub definicji sugeruje, że producent musi przynajmniej do pewnego stopnia przewidzieć zamierzone zastosowanie projektu i być może ograniczyć obszary dopuszczalne użycie przy wejściu na rynek amerykański. Z drugiej strony, wymogi regulacyjne UE można traktować jako podstawę dla obowiązków, które należy spełnić, mając do czynienia z danymi osobowymi lub z niektórymi operatorami infrastruktury kluczowej. Dwa akty prawne UE kierujące rozwojem i utrzymaniem systemów informatycznych to ogólne rozporządzenie o ochronie danych (RODO)2 oraz dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa NIS)3. RODO może mieć pewne drobne różnice między państwami członkowskimi, ale stanowi podstawę jednolitego jednolitego rynku cyfrowego w Unii Europejskiej. Jako dyrektywa, NIS będzie prawdopodobnie różnie przyjmowany przez państwa członkowskie, chociaż określa, co można uznać za minimalny poziom odpowiedzialności za bezpieczeństwo systemów informatycznych.

Ogólne rozporządzenie o ochronie danych

Intencją RODO jest wzmocnienie i doprecyzowanie praw w odniesieniu do danych osobowych osób fizycznych – czyli osób zamieszkałych na terenie Unii Europejskiej. RODO dotyczy organizacji na całym świecie, jeśli zamierzeni użytkownicy pochodzą z Unii Europejskiej i przetwarzane są dane osobowe. Firma, w przypadku której stwierdzono naruszenie przepisów, może zostać obciążona wysokimi grzywnami i opłatami odszkodowawczymi dla osób, których dane dotyczą (art. 82 i 83 RODO). Przepisy rozdzielają rolę administratora i podmiotu przetwarzającego jako różne podmioty prawne. Administrator zbiera wstępną zgodę lub umowę i nie może przenieść odpowiedzialności w stosunku do osoby, której dane dotyczą, na osobę trzecią. Nawet jeśli podmiot przetwarzający ma miejsce zamieszkania w kraju spoza Unii Europejskiej, podmiot przetwarzający nadal jest związany RODO podczas przetwarzania jakichkolwiek danych osobowych dotyczących osoby w granicach UE. Jest to środek zapewniający, że transnarodowe przekazywanie danych nie narusza podstawowych praw jednostki. Dane osobowe mogą być transportowane i przetwarzane poza UE, o ile podmiot przetwarzający jest zdeterminowany przez administratora do przestrzegania RODO i że suwerenne prawo nie jest sprzeczne z prawem UE. RODO definiuje dwa rodzaje danych: dane osobowe i dane szczególnej kategorii (wrażliwe). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specjalnej kategorii. Specjalne kategorie w art. 4 ust. 1 RODO są specyficzne dla fizycznej, fizjologicznej, genetycznej, psychicznej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby fizycznej. To oddzielenie klasyfikacji danych może czasami skutkować trudnymi wyborami projektowymi. Na przykład obraz jest zaliczany do specjalnych kategorii, gdy jest używany do identyfikacji i/lub autoryzacji, podczas gdy podczas dokumentowania historii opiekuńczej ten sam obraz może być traktowany jako dane osobowe. Zakładając, że osoba, której dane dotyczą, w sposób oczywisty upubliczniła obraz poza najbliższą rodziną, system może w niektórych przypadkach zezwolić na przetwarzanie obrazu według własnego uznania. Zgodnie z art. 5 ust. 1 lit. A RODO dwie ważne koncepcje w prawodawstwie stanowią, że dane osobowe będą przetwarzane rzetelnie i w sposób przejrzysty w stosunku do osoby, której dane dotyczą. W przypadku przyjęcia IoT może to spowodować

dodatkowe wyzwania systemowe w porównaniu z dzisiejszym środowiskiem. RODO określa następujące trzy główne kwestie dotyczące sposobu osiągnięcia zgodności:

* Wymagania projektowe. Wymaganie dobrowolnie wyrażonej zgody lub; na podstawie umowy lub w celu wykonania umowy; minimalizacja danych; ochrona danych w fazie projektowania i domyślna.

* Postępowanie z danymi osobowymi. Dostęp; sprostowanie; ruchliwość; przejrzystość użytkowania; skasowanie.

* Ograniczenia przetwarzania. Powiadomienie; ograniczenie; bezpieczeństwo.

Rozważmy metodę integracji sprzętu i usług/platform IoT jako tradycyjnego procesu analizy danych. Jakość danych z generatorów danych, takich jak czujniki, musi w świetle RODO być dokładna i niezawodna. Metainformacje opisujące np. źródło danych, prawa dostępu i uzasadnienie zgodnego z prawem przetwarzania powinny być rejestrowane wraz z danymi, gdy zostaną powiązane z osobą fizyczną. Podczas inżynierii funkcji należy dołożyć starań, aby statystyki opisowe nie naruszały integralności osoby, której dane dotyczą, ani nie wprowadzały nowych funkcji, które można uznać za wrażliwe. Przykładem nowej funkcji jest grupowanie oparte na lokalizacji i dodatkowych informacjach, takich jak miejsce kultu, które można uznać za wywnioskowanie o religii i/lub rasie. Jeżeli takie statystyki są potrzebne do określenia czynników i/lub przyczyn w celu ustalenia hipotezy, wówczas wysiłki te należy wcześniej ujawnić osobie, której dane dotyczą. Potrzebę przejrzystego przetwarzania i przejrzystego przesyłania/manipulacji/usuwania danych najlepiej może zaspokoić niezmienne rozwiązanie do przechowywania danych, takie jak technologia oparta na księgach, taka jak blockchain. Traktowanie każdej odpowiadającej operacji jako transakcji i definiowanie inteligentnego kontraktu dla tej operacji zapewnia rejestrację podlegającą kontroli do celów śledczych oraz podejście do wykazania zgodności potencjalnym użytkownikom i organowi regulacyjnemu.

Dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych

Dyrektywa NIS jest nieco bardziej restrykcyjna w swoim zastosowaniu niż RODO. Intencją NIS jest to, aby nie nakładać dodatkowego obciążenia na małe i średnie przedsiębiorstwa, ale raczej stanowić zalecenie dotyczące postępowania w przypadku incydentów związanych z bezpieczeństwem. Należy zauważyć, że postępowanie w przypadku incydentów bezpieczeństwa dotyczących danych osobowych lub danych sektorowych może zostać doprecyzowane w RODO lub innych odpowiednich aktach sektorowych. Incydenty są definiowane jako wszelkie zdarzenia mające rzeczywisty negatywny wpływ na bezpieczeństwo sieci i systemów informatycznych. Przedsiębiorstwa, które mieszczą się w definicji dyrektywy, a tym samym muszą wypełniać swoje obowiązki, to operatorzy podstawowych usług, takich jak energia, woda, transport, bankowość, infrastruktura rynków finansowych, opieka zdrowotna i infrastruktura cyfrowa. Wymagania tych przedsiębiorstw w zakresie środków bezpieczeństwa są następujące:

* Zapobieganie zagrożeniom. Odpowiednie i proporcjonalne do ryzyka środki techniczne i organizacyjne.

* Zapewnienie bezpieczeństwa IT. Zapewnij poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do zagrożeń.

* Obsługa incydentów. Zapobiegaj i minimalizuj wpływ incydentów na systemy informatyczne wykorzystywane do świadczenia usług.

Druga kategoria zdefiniowana przez NIS, oprócz głównych operatorów, obejmuje dostawców usług cyfrowych, takich jak internetowe platformy handlowe, usługi przetwarzania w chmurze i

wyszukiwarki. Obowiązki firm należących do tej kategorii są nieco rozszerzone i oprócz przedstawionych powyżej wymagań dla operatorów kluczowych, te dodatkowe środki obejmują zarządzanie ciągłością działania; monitorowanie, audyt i testowanie; i zgodność z międzynarodowymi standardami.

Technologia Blockchain

Technologia Blockchain została wprowadzona przez Nakamoto (2008) jako platforma dla kryptowaluty Bitcoin. Blockchain to rozproszona baza danych do przechowywania stale rosnącej listy rekordów zwanych blokami. Łańcuch bloków jest replikowany w sieci węzłów peer-to-peer, w której każdy węzeł przechowuje kopię całej bazy danych. Topologia łańcucha bloków to łańcuch bloków, ponieważ każdy blok poza pierwszym blokiem, tzw. Genesis Block, zawiera link do poprzedniego bloku zaimplementowany jako hash poprzedniego bloku. Każdy blok w łańcuchu bloków ma również znacznik czasu. Użytkownik łańcucha bloków jest właścicielem węzła w sieci łańcucha bloków do operacji na łańcuchu bloków i musi również posiadać unikalną parę kluczy w kryptografii klucza publicznego. Klucz publiczny identyfikuje użytkownika łańcucha bloków. Użytkownik łańcucha bloków działa na łańcuchu bloków z węzła w sieci łańcucha bloków. Operacja na łańcuchu bloków to transakcja zainicjowana przez użytkownika łańcucha bloków. Transakcja tworzy zapis, na przykład, o transferze bitcoinów, danych, własności fizycznej lub innego zasobu od użytkownika blockchain do innego użytkownika tego samego blockchain. Rekord transakcji jest podpisany przez użytkownika blockchain, który zainicjował transakcję i jest wysyłany do wszystkich węzłów sieci blockchain. Każdy węzeł sieci blockchain próbuje zweryfikować odebrany rekord transakcji za pomocą klucza publicznego inicjatora powiązanej transakcji. Rekordy transakcji, których nie można zweryfikować przez wszystkie węzły sieci blockchain, są uważane za nieprawidłowe i są odrzucane. Specjalne węzły sieci blockchain zwane węzłami górniczymi zbierają zweryfikowane rekordy transakcji i przechowują je jako listy w blokach kandydujących ze znacznikami czasu. Węzeł wydobywający wykonuje rozproszony proces oceny obliczeniowej, zwany wydobywaniem, na swoim bloku kandydującym, zanim będzie mógł zostać połączony z łańcuchem bloków. Istnieje kilka implementacji kopania dla blockchainów. W blockchainie Bitcoina kopanie opiera się na dowodach pracy (PoW). Oznacza to, że każdy węzeł górniczy wielokrotnie tworzy skrót konkatenacji ostatniego bloku blockchain i nowego jednorazowego (losowo wybrana wartość), dopóki nie zostanie utworzony skrót o wymaganym stopniu trudności. Tworzone skróty są różne, ponieważ w każdym z nich nonce jest inny. Węzeł górniczy, który najpierw tworzy hash o wymaganej trudności, może połączyć swój kandydujący blok z łańcuchem bloków. Wymagana trudność jest określona przez liczbę wiodących bitów zerowych w utworzonym hashu. Na przykład, jeśli trudność wynosi 10 bitów zerowych, potrzeba średnio 210 prób, aż do utworzenia skrótu wymaganej trudności. W ten sposób węzeł wydobywczy o największej mocy przetwarzania połączy swój kandydujący blok z łańcuchem bloków z największym prawdopodobieństwem. W blockchainie Bitcoin trudność PoW zwiększa się po 2 tygodniach, aby kontrolować tempo wzrostu blockchain. Łańcuch bloków może być publiczny, dozwolony lub prywatny. Całe oprogramowanie publicznego łańcucha bloków jest oprogramowaniem typu open source. Każdy może skorzystać z publicznego łańcucha bloków, na przykład łańcucha bloków Bitcoin, dołączając do sieci blockchain. Użytkownik dołącza do sieci blockchain, kopiując cały blockchain i instalując oprogramowanie blockchain na własnym węźle. Każdy użytkownik blockchain może również posiadać węzeł wydobywczy, na przykład instalując oprogramowanie wydobywcze na własnym węźle w sieci blockchain. Nowsze implementacje blockchain, które rozszerzają funkcjonalność oferowaną przez blockchain Bitcoin, są określane jako Blockchain 2.0. Jedną z interesujących funkcji Blockchain 2.0 jest wsparcie dla inteligentnych kontraktów, które jako koncepcję wprowadził Szabo (1997). Inteligentna umowa to program komputerowy, który zawiera warunki umowy, które umożliwiają weryfikację, negocjowanie lub egzekwowanie umowy. Przykładem platformy blockchain skupionej na inteligentnych kontraktach jest

Ethereum5, której kryptowaluta nazywa się Ether. Inteligentna umowa w Ethereum nazywa się DApp (Zdecentralizowana aplikacja), która może być wykonywana na serwerze lub bezpośrednio w węźle Ethereum. Zobacz na przykład Tapscott i Tapscott (2016), aby uzyskać szczegółowy opis technologii blockchain i aplikacji blockchain. Bezpieczeństwo blockchainu opiera się na współzależności haszowej pomiędzy kolejnymi blokami w połączeniu z dystrybucją kopii całego blockchaina do wszystkich węzłów w sieci blockchain. Łańcuch bloków jest w praktyce odporny na manipulacje – to znaczy odporny na próby modyfikacji – ponieważ blok nie może zostać zmieniony bez zmiany wszystkich kolejnych bloków i udziału całej sieci w weryfikacji i rejestrowaniu zmian. Co więcej, blockchain nie jest kontrolowany przez żaden pojedynczy scentralizowany organ, który mógłby być celem ataku, ponieważ kompletne kopie blockchain są przechowywane we wszystkich węzłach sieci peer-to-peer. Jeśli jednak atakujący może uzyskać kontrolę nad wystarczającą liczbą węzłów w sieci blockchain typu peer-to-peer, w tym nad niektórymi węzłami górniczymi, wówczas może dojść do utraty danych i/lub wstawienia uszkodzonych danych do zaatakowanego łańcucha bloków. Przykładami ataków bezpieczeństwa na blockchainy są samolubny atak wydobywczy , atak rewizji historii , atak zaćmienia i uporczywy atak wydobywczy . Złośliwe węzły wydobywcze nie przesyłają wszystkich wykopanych nowych bloków do walidacji w sieci blockchain w samolubnym ataku górniczym. Złośliwy górnik mający ponad dwa razy większą moc obliczeniową niż wszystkie uczciwe węzły wydobywcze razem, może wstawić uszkodzone bloki do łańcucha bloków w ataku polegającym na rewizji historii. Wszystkie połączenia przychodzące i wychodzące węzła docelowego w sieci blockchain są kontrolowane w ataku zaćmienia. Uparty atak górniczy łączy samolubne wydobycie z atakiem zaćmienia.

Blockchainy i systemy IoT

Urządzenia IoT generują ogromne ilości danych, które muszą być przechowywane i przetwarzane. Każda operacja CRUD (Create, Read, Update lub Delete) na danych IoT może zostać zarejestrowana jako rekord transakcji w bloku blockchain. W związku z tym mogą zostać wykryte nieautoryzowane operacje na przechowywanych danych IoT. Poświadczenia tożsamości dla urządzenia IoT można zarejestrować jako rekord transakcji w bloku blockchain podczas produkcji urządzenia i pobrać później, gdy urządzenie jest w trakcie używania. Reguły dostępu dla urządzeń IoT można określać i egzekwować za pomocą inteligentnych kontraktów. Dlatego też mogą zostać wykryte nieautoryzowane operacje na przechowywanych danych IoT. Do ochrony danych IoT, które można bezpiecznie przechowywać w różnych węzłach sieci, nie jest potrzebny scentralizowany organ, taki jak dostawca pamięci masowej w chmurze, gdy łańcuch bloków gwarantuje autentyczność danych i zapobiega nieautoryzowanemu dostępowi. Historia wdrożenia urządzenia IoT może być przechowywana jako rekordy transakcji w blockchain. Rekordy transakcji mogą być przechowywane w blokach łańcucha bloków, gdy urządzenie IoT jest produkowane, dostarczane właścicielowi, instalowane, aktualizowane i dostarczane innemu właścicielowi i tak dalej. Blockchain może również umożliwić bezpieczne przesyłanie wiadomości między urządzeniami IoT. Wymianę wiadomości między urządzeniami IoT można traktować podobnie do transakcji finansowych w sieci Bitcoin. Wymianę wiadomości między urządzeniami IoT można włączyć za pomocą inteligentnych kontraktów, które wdrażają umowy między dwiema stronami. Podstawową funkcją łańcucha bloków jest to, że utrzymywana jest należycie zdecentralizowana, zaufana księga wszystkich transakcji w sieci. Ta funkcja może zapewnić wiele zgodności i wymagań prawnych dla systemów IoT, na przykład w RODO.

Przykłady rozwiązań bezpieczeństwa opartych na Blockchain dla systemów IoT

Zdecentralizowane i autonomiczne funkcje łańcucha bloków sprawiają, że jest on niemal idealnym elementem rozwiązań bezpieczeństwa IoT. Wykorzystanie Blockchain może zapewnić poziom bezpieczeństwa IoT, który w innym przypadku byłby trudny lub nawet niemożliwy do osiągnięcia. W

tej sekcji przedstawiono niektóre z ostatnio proponowanych rozwiązań bezpieczeństwa IoT, które są oparte na technologii blockchain.

Bezpieczne zarządzanie urządzeniami IoT

Zarządzanie urządzeniem IoT obejmuje kontrolę ustawień konfiguracyjnych i trybów pracy, a także zapewnienie nieprzerwanej pracy. Kontrola ustawień konfiguracji i trybów działania oparta na technologii Blockchain może zapobiegać nieautoryzowanym próbom dostępu, a także zapewniać ochronę przed atakami typu „odmowa usługi". Huh , zaproponował sterowanie i konfigurację urządzeń IoT wykorzystujących Ethereum jako platformę blockchain. Poświadczenie identyfikacyjne dla urządzenia IoT może być zaimplementowane za pomocą unikalnej pary kluczy (tj. klucza prywatnego i klucza publicznego) w kryptografii klucza publicznego. Klucz prywatny jest przechowywany w urządzeniu IoT, podczas gdy klucz publiczny jest zarejestrowany jako rekord transakcji w bloku Ethereum. Urządzenie IoT można następnie zaadresować w sieci Ethernet za pomocą swojego klucza publicznego. Ethereum zostało wybrane jako platforma blockchain, ponieważ jego inteligentne kontrakty umożliwiają wykonywanie programów na blockchain. Zachowanie urządzeń IoT można zatem zaprogramować w inteligentnych kontraktach. Na potwierdzenie zaproponowanej koncepcji przeprowadzono symulację na systemie złożonym z trzech urządzeń IoT: licznika energii elektrycznej, żarówki LED i klimatyzatora. Za pomocą smartfona ustanowiono politykę, zgodnie z którą klimatyzator i żarówka przechodzą w tryb oszczędzania energii, jeśli pomiar licznika przekracza 150 kW. W przypadku licznika zaprogramowano inteligentną umowę do wysyłania wartości pomiarowych i danych uwierzytelniających (tj. klucza publicznego i podpisu) do Ethereum. Zaprogramowano również inteligentne kontrakty dla klimatyzatora i żarówki. Te kontrakty pobierały wartości pomiarowe z powiązanymi danymi uwierzytelniającymi tożsamość z Ethereum. Poświadczenia tożsamości potwierdziły, że odczytana wartość pomiarowa była wartością licznika, a przejście do trybu oszczędzania energii nastąpiło po przekroczeniu progu 150kW odczytanej wartości.

Bezpieczne aktualizacje oprogramowania sprzętowego w urządzeniach IoT

Dostawcy urządzeń IoT zdalnie aktualizują oprogramowanie sprzętowe dostarczonych urządzeń w celu zainstalowania nowych funkcji i załatania wykrytych luk. Aktualizacje te są zwykle pobierane na podstawie żądań klientów z serwera repozytorium zawierającego wstępnie skompilowane pliki binarne oprogramowania układowego zabezpieczone przez podpisane skróty komunikatów infrastruktury klucza publicznego (PKI). Skrót podpisanej wiadomości i publiczny klucz podpisu są dołączone do pobranego pliku oprogramowania układowego. Aktualizacja oprogramowania układowego na urządzeniu IoT rozpoczyna się tylko wtedy, gdy pomyślne jest sprawdzenie zabezpieczeń za pomocą pobranego klucza publicznego. Jednak ten protokół aktualizacji oprogramowania układowego klient-serwer generuje zbyt duży ruch w sieci, jeśli miliony urządzeń IoT jednocześnie żądają aktualizacji. Zaproponowano rozwiązanie wykorzystujące łańcuchy bloków do bezpiecznej aktualizacji oprogramowania układowego w urządzeniach IoT, w którym globalny ruch sieciowy do serwera jest zastępowany głównie lokalną komunikacją peer-to-peer między węzłami sieci blockchain. W tym rozwiązaniu producent urządzeń IoT przechowuje skróty wydanych wersji oprogramowania układowego w łańcuchu bloków, który jest dostępny dla wszystkich dostarczonych urządzeń IoT. Christidis i Devetsikiotis zasugerowali, że korzystając z preinstalowanej inteligentnej umowy z warunkiem wielokrotnego sprawdzania po upływie określonego czasu, czy dostępna jest nowa wersja oprogramowania układowego, urządzenie IoT może autonomicznie dowiadywać się o nowych wersjach oprogramowania układowego. Urządzenie IoT może pobrać skrót wydanego oprogramowania układowego z blockchain6 i użyć go do bezpiecznego pobrania nowej wersji oprogramowania układowego z rozproszonego systemu plików peer-to-peer składającego się z węzła producenta i urządzeń IoT z zainstalowanymi wersjami oprogramowania układowego. Skróty

oprogramowania układowego przechowywane w łańcuchu bloków można również wykorzystać do sprawdzenia, czy oprogramowanie układowe zainstalowane na urządzeniach IoT jest nienaruszone. We wspomnianym rozwiązaniu wszystkie urządzenia IoT dostarczane przez tego samego dostawcę są normalnymi węzłami blockchain. Inne węzły łańcucha bloków to węzły weryfikacyjne, które są obsługiwane przez dostawcę oprogramowania układowego za pośrednictwem bezpiecznego połączenia sieciowego w celu utrzymania zaktualizowanego oprogramowania układowego i metadanych oprogramowania układowego. Urządzenie IoT rozgłasza żądania aktualizacji oprogramowania układowego do węzłów łańcucha bloków. Jeśli odpowiedź zostanie po raz pierwszy odebrana z węzła weryfikacji, a oprogramowanie układowe urządzenia IoT jest aktualne, oprogramowanie układowe jest weryfikowane. W przeciwnym razie najnowsze oprogramowanie układowe jest pobierane z odpowiadającego węzła weryfikacji. Jeśli odpowiedź zostanie po raz pierwszy odebrana z normalnego węzła blockchain, który ma tę samą wersję oprogramowania układowego, co urządzenie IoT żądające aktualizacji oprogramowania układowego, wersja oprogramowania układowego jest weryfikowana przez uproszczoną procedurę wyszukiwania PoW, w której wystarczy sześć odpowiedzi dziennika weryfikacji. W przeciwnym razie aktualne oprogramowanie układowe jest pobierane z węzła weryfikacji na urządzenie IoT – normalny węzeł łańcucha bloków – którego wersja oprogramowania układowego jest starsza. Każdy blok łańcucha bloków składa się z nagłówka i pola weryfikacyjnego, które składa się z licznika weryfikacji, skrótów wszystkich przechowywanych transakcji, dziennika weryfikacji, nazwy węzła sieci blockchain, bieżącej wersji oprogramowania układowego i skrótu pliku oprogramowania układowego. Dziennik weryfikacji zawiera sygnatury czasowe reprezentujące czasy weryfikacji i identyfikatory węzłów sieci, które żądają aktualizacji oprogramowania układowego, oraz identyfikatory węzłów sieci, które odpowiadają na takie żądania.

Ocena zaufania zaufanej bazy obliczeniowej w urządzeniach IoT

Trusted Computing Base (TCB) to zestaw sprzętu, oprogramowania układowego i/lub składników oprogramowania, które zapewniają bezpieczeństwo systemu komputerowego. Oznacza to, że aby złamać zabezpieczenia, atakujący musi obalić jeden lub więcej z tych komponentów. TCB może zatem być częścią urządzenia IoT, czyli małego systemu komputerowego. TCB jest godna zaufania, jeśli wszystkie elementy TCB są niezmienione przez błędy i nienaruszone przez przeciwników. Pomiar TCB, który tworzy skróty wszystkich składników TCB, jest przeprowadzany w celu oceny wiarygodności TCB. Jeśli te skróty są bezpiecznie przechowywane, można je później wykorzystać do weryfikacji TCB. Pomiary TCB są przeprowadzane, gdy urządzenie IoT jest podłączone do Internetu i za każdym razem, gdy jego TCB jest aktualizowane. Wiarygodność została naruszona, jeśli nie można zweryfikować pomiaru TCB. Weryfikator dokonuje zdalnej atestacji, wydając kryptograficzny numer jednorazowy i podpisując konkatenację zweryfikowanego pomiaru TCB z identyfikatorem jednorazowym, aby upewnić się, że TCB urządzenia IoT jest godny zaufania. W firmie Park and Kim opracowano protokół o nazwie TM-Coin (TCB Measurement-Coin) w celu wiarygodnego zarządzania pomiarami TCB w urządzeniach IoT. TM-Coin tworzy rekordy transakcji zweryfikowanych pomiarów TCB i przechowuje te rekordy w blokach blockchain. TM-Coin wykorzystuje środowisko Trusted Execution Environment (TEE) dostarczane przez ARM TrustZone7 jako bazę TCB w urządzeniach IoT do bezpiecznego generowania rekordów transakcji dla łańcucha bloków. Protokół TM-Coin składa się z dwóch typów transakcji blockchain: rejestracji i aktualizacji. Transakcja rejestracji przechowuje zapis weryfikacji pomiaru TCB w bloku blockchain po podłączeniu urządzenia IoT. Po aktualizacji kodu co najmniej jednego komponentu TCB w urządzeniu IoT aktualizacja transakcji przechowuje również zapis weryfikacji pomiaru TCB w bloku blockchain. Węzły górnicze w łańcuchu bloków wykonują zdalną atestację TCB w urządzeniu IoT podczas transakcji. Dane wykryte przez urządzenie IoT mają pewność,

że są godne zaufania po zdalnym poświadczeniu przez zewnętrznego weryfikatora. Funkcja poświadczania to

sign(hash (TCB_M, D, N))

gdzie TCB_M to ostatni pomiar TCB urządzenia IoT uzyskany z łańcucha bloków, D to dane wykryte przez urządzenie, a N to jednorazowa wartość wydana przez weryfikatora.

Weryfikacja tożsamości urządzeń IoT

Bezpieczną tożsamość urządzenia IoT można zaimplementować jako klucz prywatny we wbudowanym chipie kryptograficznym z kluczem publicznym. Odpowiedni klucz publiczny jest przechowywany w bloku blockchain przez producenta urządzenia IoT. Węzeł sieci zaczyna uzyskiwać dostęp do urządzenia IoT za pomocą losowego komunikatu wezwania, który jest zwracany przez urządzenie IoT z sygnaturą. Węzeł sieci uzyskujący dostęp może następnie zweryfikować tożsamość urządzenia IoT za pomocą klucza publicznego, który można pobrać z łańcucha bloków. Tożsamość urządzenia IoT, która jest weryfikowana przy użyciu łańcucha bloków, umożliwia niemal całkowicie bezpieczne uwierzytelnianie IoT, prawie uniemożliwia fałszowanie tożsamości i zapewnia integralność danych przechwyconych z urządzeń IoT ze względu na odporność łańcucha bloków na manipulacje. Tożsamość urządzenia IoT, która jest weryfikowana przy użyciu łańcucha bloków, została zaproponowana do użycia do utworzenia dziennika tożsamości opartego na łańcuchu bloków, przechwytującego identyfikator urządzenia, jego producenta, listy dostępnych aktualizacji oprogramowania układowego i znane problemy z bezpieczeństwem . Historia urządzenia z bezpiecznie zweryfikowaną tożsamością może być również śledzona przez blockchain. Historia zaczyna się, gdy producent przechowuje tożsamość – klucz publiczny – wyprodukowanego urządzenia IoT w bloku blockchain. Tożsamości, które są weryfikowane za pomocą łańcucha bloków, są opracowywane dla urządzeń IoT, takich jak kamery monitorujące.

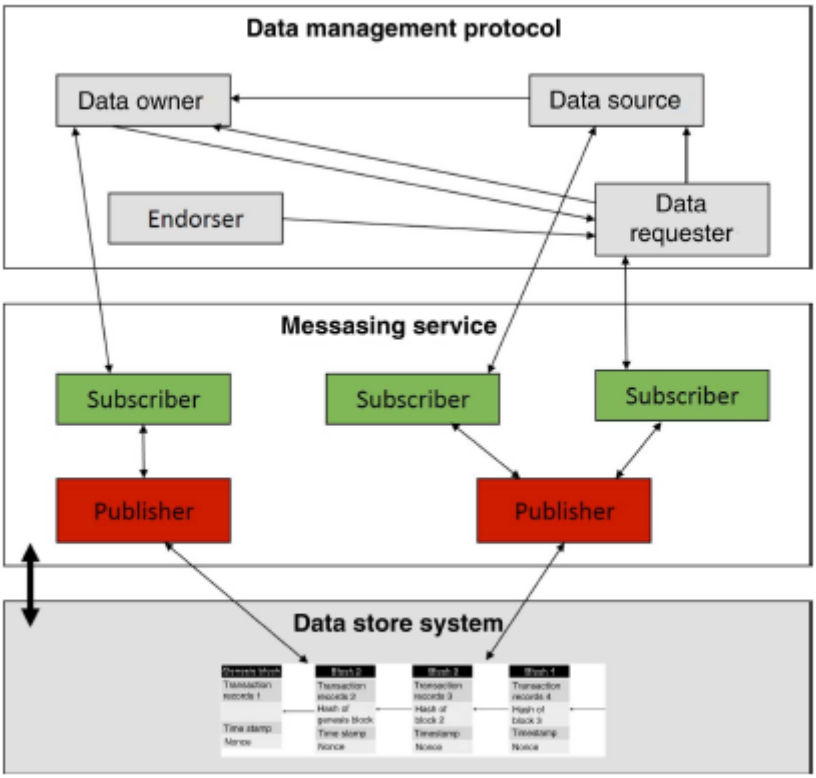
Bezpieczny system przechowywania danych do informacji kontroli dostępu

Obecne standardowe rozwiązania kontroli dostępu do urządzeń podłączonych do sieci opierają się na listach kontroli dostępu (ACL). Jednak niemożliwe byłoby utrzymanie listy ACL dla każdego urządzenia IoT i poleganie na scentralizowanych serwerach kontroli dostępu, gdy IoT skaluje się do miliardów urządzeń i milionów właścicieli urządzeń. Aby zapewnić tym właścicielom urządzeń IoT kontrolę nad danymi generowanymi przez ich urządzenia, wdrożenie blockchain jest możliwym rozwiązaniem, które wyklucza zależność od scentralizowanych stron trzecich. Oparty na blockchain bezpieczny system przechowywania danych do informacji kontroli dostępu został wprowadzony jako komponent proponowanego rozwiązania w celu ochrony kontroli dostępu właścicieli urządzeń IoT do danych generowanych przez ich urządzenia IoT. Pozostałe składniki to protokół zarządzania danymi i usługa przesyłania wiadomości. Proponowane rozwiązanie implementuje kontrolę dostępu opartą na rolach i możliwościach. Gdy strona ze zdefiniowaną rolą wysyła komunikat kontroli dostępu do innej strony również ze zdefiniowaną rolą, wiadomość jest dostarczana do usługi przesyłania wiadomości. Usługa przesyłania wiadomości wysyła wiadomość do systemu przechowywania danych, gdzie jest przechowywana jako rekord transakcji w bloku blockchain. Następnie strona odbierająca pobiera wiadomość z bloku blockchain w systemie przechowywania danych za pośrednictwem usługi przesyłania wiadomości. Zdefiniowano cztery role, jak pokazano na Rysunku 9.2: właściciel danych, źródło danych, osoba żądająca danych i osoba zatwierdzająca. Właściciel danych jest właścicielem i udziela dostępu do danych generowanych przez jego urządzenia IoT (tj. źródła danych). Żądający danych (np. urządzenie IoT) żąda dostępu do danych IoT, a osoba wspierająca zatwierdza takie żądania. Protokół zarządzania danymi to protokół wymiany komunikatów służący do kontroli dostępu opartej na możliwościach. Możliwość umożliwia żądającemu danych dostęp do obiektu danych właściciela danych w źródle danych. Protokół zarządzania danymi składa się z pięciu typów komunikatów kontroli

dostępu: komunikat generowania biletu źródła danych, komunikat żądania danych, komunikat wymiany biletu, komunikat dostępu do danych i komunikat ogłoszenia dostępu. System przechowywania danych to łańcuch bloków podobny do łańcucha bloków Bitcoin. Usługa przesyłania wiadomości przechowuje wiadomości otrzymane od nadawcy jako rekordy transakcji w blokach blockchain w systemie przechowywania danych i implementuje protokół wydawca-subskrybent - w celu dostarczania wiadomości przechowywanych jako rekordy transakcji w blokach blockchain w systemie przechowywania danych.

Bezpieczny system przechowywania danych do informacji kontroli dostępu

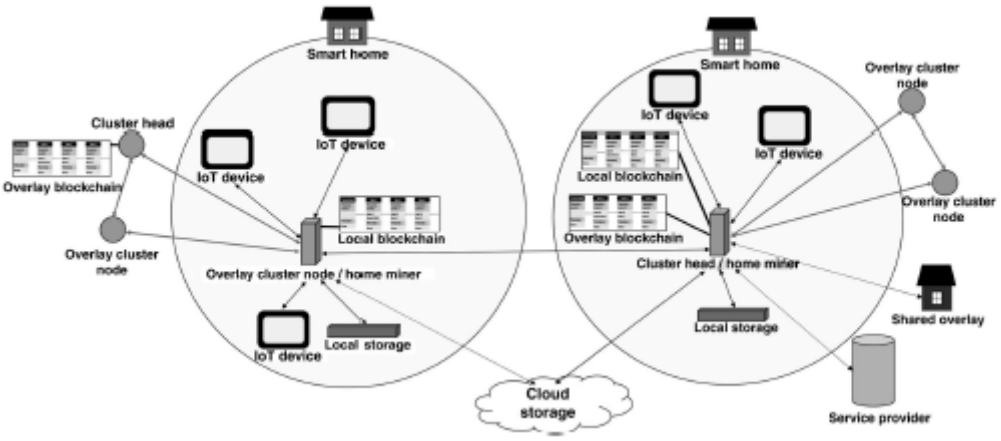
Obecne standardowe rozwiązania kontroli dostępu do urządzeń podłączonych do sieci opierają się na listach kontroli dostępu (ACL). Jednak niemożliwe byłoby utrzymanie listy ACL dla każdego urządzenia IoT i poleganie na scentralizowanych serwerach kontroli dostępu, gdy IoT skaluje się do miliardów urządzeń i milionów właścicieli urządzeń. Aby zapewnić tym właścicielom urządzeń IoT kontrolę nad danymi generowanymi przez ich urządzenia, wdrożenie blockchain jest możliwym rozwiązaniem, które wyklucza zależność od scentralizowanych stron trzecich. Oparty na blockchain bezpieczny system przechowywania danych do informacji kontroli dostępu został wprowadzony jako komponent proponowanego rozwiązania w celu ochrony kontroli dostępu właścicieli urządzeń IoT do danych generowanych przez ich urządzenia IoT. Pozostałe składniki to protokół zarządzania danymi i usługa przesyłania wiadomości. Proponowane rozwiązanie implementuje kontrolę dostępu opartą na rolach i możliwościach. Gdy strona ze zdefiniowaną rolą wysyła komunikat kontroli dostępu do innej strony również ze zdefiniowaną rolą, wiadomość jest dostarczana do usługi przesyłania wiadomości. Usługa przesyłania wiadomości wysyła wiadomość do systemu przechowywania danych, gdzie jest przechowywana jako rekord transakcji w bloku blockchain. Następnie strona odbierająca pobiera wiadomość z bloku blockchain w systemie przechowywania danych za pośrednictwem usługi przesyłania wiadomości. Przegląd proponowanego rozwiązania przedstawiono na rysunku 9.2. Zdefiniowano cztery role, jak pokazano na Rysunku:



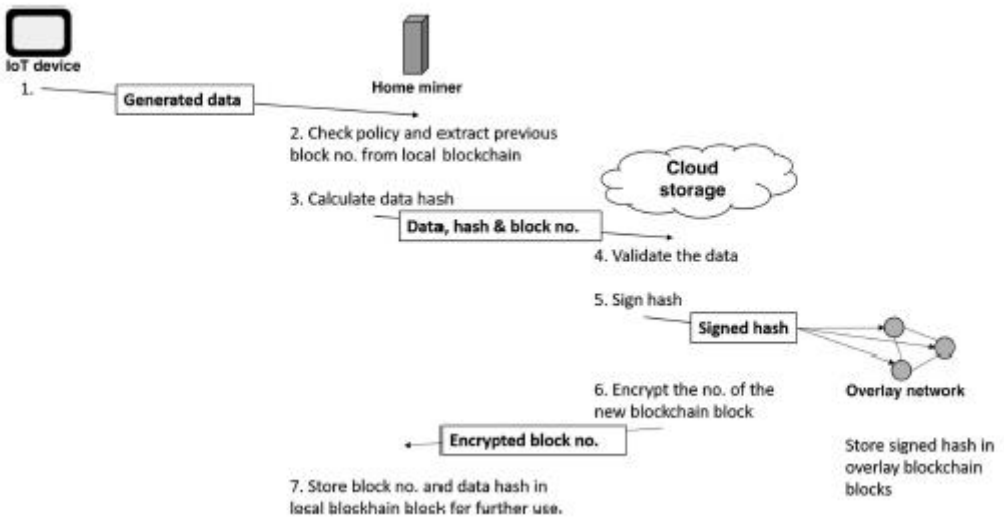
właściciel danych, źródło danych, osoba żądająca danych i osoba zatwierdzająca. Właściciel danych jest właścicielem i udziela dostępu do danych generowanych przez jego urządzenia IoT (tj. źródła danych). Żądający danych (np. urządzenie IoT) żąda dostępu do danych IoT, a osoba wspierająca zatwierdza takie żądania. Protokół zarządzania danymi to protokół wymiany komunikatów służący do kontroli dostępu opartej na możliwościach. Możliwość umożliwia żądającemu danych dostęp do obiektu danych właściciela danych w źródle danych. Protokół zarządzania danymi składa się z pięciu typów komunikatów kontroli dostępu: komunikat generowania biletu źródła danych, komunikat żądania danych, komunikat wymiany biletu, komunikat dostępu do danych i komunikat ogłoszenia dostępu. System przechowywania danych to łańcuch bloków podobny do łańcucha bloków Bitcoin. Usługa przesyłania wiadomości przechowuje wiadomości otrzymane od nadawcy jako rekordy transakcji w blokach łańcucha bloków w systemie przechowywania danych i implementuje protokół wydawca-subskrybent — jak pokazano na rysunku — w celu dostarczania wiadomości przechowywanych jako rekordy transakcji w blokach łańcucha bloków w magazynie danych system.

Architektura bezpieczeństwa oparta na blockchain dla urządzeń IoT w inteligentnych domach

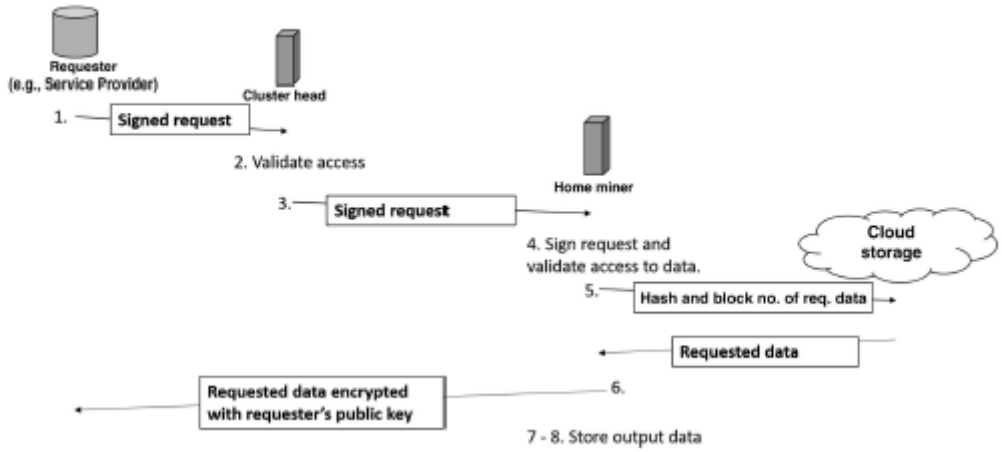
Zaproponowano architekturę opartą na blockchain dla sieci lokalnych w inteligentnych domach (lub w niektórych innych środowiskach lokalnych) z wieloma podłączonymi urządzeniami IoT, takimi jak inteligentne termostaty, inteligentne żarówki i kamery IP. Architektura ma trzy poziomy, a mianowicie sieci lokalne w inteligentnych domach, sieć nakładkową i przechowywanie w chmurze. Na każdym poziomie podmioty wykorzystują transakcje blockchain do wzajemnej komunikacji. Typy transakcji obejmują transakcje genezy, transakcje sklepu, transakcje dostępu i monitorowanie transakcji. Architektura, którą przedstawiono na rysunku, zapewnia silną ochronę przed atakami typu „odmowa usługi”, atakami modyfikującymi, atakami typu drop, atakami typu mining, atakami dołączającymi i atakami typu „linking”.



W sieci lokalnej istnieje prywatny lokalny łańcuch bloków, który jest przechowywany, wydobywany i zarządzany przez co najmniej jedno urządzenie. Gdy nowe urządzenie IoT jest podłączone do sieci lokalnej, rekord transakcji genesis jest przechowywany w lokalnym bloku blockchain. Po usunięciu istniejącego urządzenia IoT jego księga jest usuwana z lokalnego łańcucha bloków. Ten lokalny łańcuch bloków ma nagłówek polityki zawierający listę kontroli dostępu, która umożliwia właścicielowi sieci lokalnej kontrolę nad wszystkimi transakcjami łańcucha bloków w sieci lokalnej. Komunikacja między urządzeniami IoT jest szyfrowana za pomocą wstępnie udostępnionych kluczy Diffie-Hellman8. Sieć lokalna może mieć lokalną pamięć masową na dane. Urządzenie górnicze utrzymuje listę kluczy publicznych reprezentujących tożsamość cyfrową podmiotów, którym można nadać uprawnienia dostępu do danych sieci lokalnej z zewnątrz. Sieć nakładek przypomina sieć Bitcoin peer-to-peer i składa się z lokalnych urządzeń górniczych, innych lokalnych urządzeń sieciowych i / lub smartfonów lub komputerów osobistych właścicieli sieci lokalnej. Węzły sieciowe nakładek komunikują się za pośrednictwem sieci Tor, aby osiągnąć anonimowość komunikacyjna i są pogrupowane w klastry, w których dla każdego klastra wybierany jest szef klastra (CH). Każdy CH utrzymuje nakładkę blockchain i trzy listy: klucze publiczne podmiotów żądających, które mają dostęp do danych dla inteligentnych domów podłączonych do klastra, klucze publiczne takich sieci lokalnych podłączonych do klastra, do których można uzyskać dostęp z zewnątrz oraz transakcje wysyłane do inne CH. Rekordy transakcji z więcej niż jednym podpisem oraz rekordy transakcji dostępu są przechowywane w blokach nakładki blockchain. Kilka sieci lokalnych mających tego samego właściciela może być zarządzanych razem jako współdzielona nakładka składająca się ze współdzielonego łańcucha bloków ze wspólnym górnikiem i współdzieloną pamięcią masową. Urządzenia IoT w sieci lokalnej mogą przechowywać swoje dane lokalnie lub w chmurze. Magazyny w chmurze to łańcuchy bloków, w których dane IoT są przechowywane w identycznych blokach z unikalnymi numerami bloków. Lokalne urządzenie sieciowe jest uwierzytelniane w chmurze przez podany numer bloku i skrót przechowywanych danych. Transakcja przechowywania, zilustrowana na rysunku , jest inicjowana przez urządzenie IoT w sieci lokalnej w celu przechowywania wygenerowanych danych, na przykład przez termostat do przechowywania pomiarów temperatury w chmurze.



Transakcja dostępu przedstawiona na rysunku może zostać zainicjowana przez właściciela sieci lokalnej lub dostawcę usług w celu pobrania przechowywanych danych IoT.



Transakcja monitorowania, którą może zainicjować właściciel sieci lokalnej, pobiera stan podłączonego urządzenia IoT, taki jak aktualna wartość temperatury termostatu.

Zwiększona niezawodność medycznych urządzeń IoT

Medyczne urządzenia IoT podlegają tym samym problemom bezpieczeństwa, co inne urządzenia IoT. Bezpieczeństwo użytkowników w medycznych systemach opartych na IoT jest najwyższym priorytetem. Użytkownik musi być chroniony przed awarią systemu spowodowaną awarią urządzenia lub incydentem bezpieczeństwa. Medyczne urządzenie IoT musi działać niezawodnie i opierać się atakom bezpieczeństwa. Ponadto należy zapewnić integralność i prywatność użytkownika danych generowanych przez medyczne systemy IoT. Wykorzystanie Blockchain w zarządzaniu medycznymi urządzeniami IoT może zapewnić ochronę przed złośliwą ingerencją w ustawienia urządzenia i tryby działania. Niezmienna księga rekordów łańcucha bloków ze zdarzeń zarządzania może zmniejszyć ryzyko awarii urządzenia. Nichol i Brandt zaproponowali wykorzystanie technologii blockchain do zarządzania urządzeniami w celu poprawy niezawodności medycznych urządzeń IoT. Gdy produkowane jest medyczne urządzenie IoT, w blok łańcucha bloków. Później dane te można

zaktualizować o dane pacjenta, szpitala, lekarza, kontakty w nagłych wypadkach i dyrektywy dotyczące opieki nad pacjentem. Pacjent i opiekunowie mogą być automatycznie powiadamiani o potrzebach serwisowych urządzenia, zbliżającym się wygaśnięciu baterii i wykrytych nieprawidłowościach zdrowotnych poprzez zestaw inteligentnych kontraktów. W związku z tym ryzyko katastrofalnej awarii urządzenia jest zmniejszane dzięki inteligentnym kontraktom wysyłającym informacje o konserwacji zapobiegawczej do pacjenta i opiekuna.

Wyzwania i przyszłe badania

Wdrożenie proponowanych rozwiązań bezpieczeństwa opartych na blockchain w IoT jest bardzo istotnym tematem dla przyszłych badań. Po pierwsze, aplikacje IoT potencjalnie korzystające z funkcji bezpieczeństwa blockchain powinny być rygorystycznie badane. Przykładem odpowiedniej domeny są aplikacje IoT w służbie zdrowia, w których manipulowanie danymi pomiarowymi dotyczącymi zdrowia może mieć katastrofalne skutki. Po ustaleniu aplikacji i ich wymagań bezpieczeństwa następnym krokiem jest ocena, w jaki sposób można wdrożyć technologię blockchain. Potrzebne są krytyczne symulacje i eksperymentalne oceny bezpieczeństwa i wydajności rozwiązań bezpieczeństwa opartych na blockchain, zanim te rozwiązania będą mogły zostać wdrożone w rzeczywistych aplikacjach. Jednocześnie wymagane są nowe, odporne na manipulacje rozwiązania bezpieczeństwa oparte na blockchain, zapewniające szczegółowe analizy śledcze dotyczące ataków na bezpieczeństwo. Dużo pracy jest również potrzebne w opracowaniu standardów projektowania sprzętu IoT, oprogramowania IoT i innego oprogramowania IoT wspierającego wdrożone i zweryfikowane rozwiązania bezpieczeństwa oparte na blockchain. Istotnym problemem przy stosowaniu rozwiązań blockchain w systemach IoT są ograniczone możliwości przetwarzania większości używanych urządzeń. Ponieważ technologia blockchain intensywnie wykorzystuje kryptografię do mieszania, podpisywania cyfrowego i szyfrowania, potrzebne są dalsze badania nad lekkimi algorytmami kryptograficznymi w celu praktycznego wdrożenia rozwiązań bezpieczeństwa opartych na blockchain.

Wnioski

Chociaż systemy IoT istniały w różnych formach od dawna, wyzwania bezpieczeństwa pojawiają się i będą pojawiać się w przewidywalnej przyszłości. Ogólne metody i narzędzia bezpieczeństwa IT nie spełniają wszystkich specyficznych wymagań dotyczących bezpiecznego wdrażania IoT. Dlatego ważna jest identyfikacja nowych metod odpowiednich dla rozwiązań bezpieczeństwa IoT. Technologia Blockchain może poprawić zdolność automatycznej reakcji na incydent bezpieczeństwa. Jest to szczególnie ważne w przypadku systemów IoT, ponieważ oczekuje się, że zdecentralizowane sieci IoT będą działać niezawodnie i bezpiecznie bez nadzoru człowieka. Istotnym zagrożeniem bezpieczeństwa dla wszystkich systemów IT, a zatem również dla systemów IoT, jest możliwość ingerencji atakujących w oprogramowanie i/lub dane rozwiązania zabezpieczającego. Rozwiązania bezpieczeństwa IoT oparte na Blockchain ograniczają to ryzyko, ponieważ są „praktycznie” odporne na manipulacje oraz ze względu na ich zdolność do przeprowadzania audytów transakcji w czasie rzeczywistym. Istnieją jednak również wady i mankamenty wykorzystania blockchain w rozwiązaniach bezpieczeństwa dla systemów IoT. Głównymi wadami urządzeń IoT o ograniczonych zasobach są rosnące wymagania dotyczące mocy obliczeniowej związane z wydobyciem PoW oraz rosnące wymagania dotyczące pamięci masowej w węzłach łańcucha bloków, gdy rozmiar księgi łańcucha bloków rośnie. Aby złagodzić te wady, należy wdrożyć inne techniki wyszukiwania, a gdy urządzenie jest zbyt ograniczone pod względem zasobów, należy prowadzić tylko księgę transakcji zależną od urządzenia. Należy zauważyć, że żadna z przedstawionych przykładów propozycji rozwiązań bezpieczeństwa IoT opartych na blockchain nie daje pełnej ochrony przed wszystkimi możliwymi zagrożeniami bezpieczeństwa i atakami. Co więcej, praktyczne wdrożenie tych rozwiązań bezpieczeństwa jest nadal kwestią przyszłości. Praktyczne rozwiązanie bezpieczeństwa dla systemu IoT może zatem łączyć wybór rozwiązań bezpieczeństwa

opartych na blockchain z zestawem innych rozwiązań bezpieczeństwa. Obecny szybki wzrost wdrożeń IoT oraz incydenty związane z bezpieczeństwem IoT, które do tej pory miały miejsce, podkreślają konieczność kontynuowania badań nad ulepszaniem zdecentralizowanych środków bezpieczeństwa i niezawodności systemów IoT.