

Г.А. ВАРДАНЯН, М.Ц. АЙВАЗЯН, О.Ж. СЕВОЯН
ПРОГРАММНО-ОПРЕДЕЛЯЕМАЯ РАДИОСИСТЕМА

Предложена новая система обработки сигналов, которая представляет собой программно-определяемую радиосистему. Все алгоритмы для обработки сигналов разработаны для программируемой логической интегральной схемы (ПЛИС). Предложенная система может использоваться как целая система для передачи и приёма сигналов (радио передатчик-приемник), которую можно контролировать с помощью программного обеспечения.

Ключевые слова: программируемая логическая интегральная схема, программно-определяемая радиосистема, цифровой сигнал, скорость передачи данных.

G.A. VARDANYAN, M.C. AYVAZYAN, O.J. SEVOYAN
SDR`SOFTWARE DEFINED RADIO SYSTEM

A new signal processing system is proposed, which is a software-defined radio system. All signal processing algorithms are designed for Field-Programmable Gate Array (FPGA). The proposed system can be used as a complete system for transmitting and receiving signals (radio transceiver), which can be controlled by software.

Keywords: Field-Programmable Gate Array (FPGA), SDR` software-defined radio, data rate.

ՀՏԴ 004.056:004.383.2

Կ.Գ. ՄԿՐՏՉՅԱՆ, Մ.Ա. ՆԱԼԲԱՆԴՅԱՆ

ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՈՒՄՆ ԱՄՊԱՅԻՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐՈՒՄ

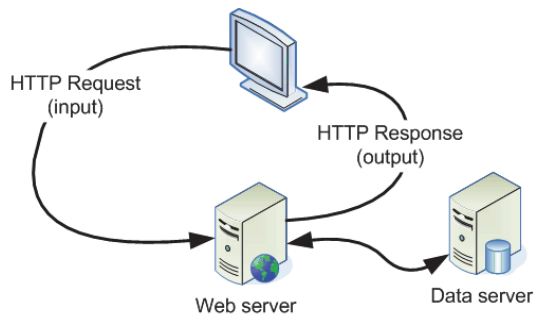
Ուսումնասիրվել են ամպային տեխնոլոգիաները, դրանց առանձնահատկությունները, կառուցվածքը, ծրագրային ապահովումը և հետագա զարգացումը: Գլխավոր խնդիրն է ապահովել համակարգի անվտանգությունը, օգտագործողների անձնական տեղեկությունների գաղտնիությունը, հասանելիությունը և այլն: Առաջարկվել է օպտիմալ լուծում տեղեկատվության անվտանգության ապահովման համար:

Առանցքային բառեր. ամպ, ամպային տեխնոլոգիա, գաղտնագրում, անվտանգություն:

Ներածություն: Թեմայի կարևորությունը պայմանավորված է այն հանգամանքով, որ արդեն մի քանի տարի է, ինչ տեղեկատվական տեխնոլոգիաների հետ առնչվող կազմակերպություններն ունեն տեղեկատվության պահպանման խնդիրներ: Հայտնի է, որ այդ խնդիրների լուծման լավագույն օրինակ են ամպային տեխնոլոգիաները [1]:

Բիզնես կիրառական ծրագրերը հարում են, այսպես կոչված, «ամպային» տեխնոլոգիաներին: Դա պատահական չէ. անցումն ավանդական ծրագրային ապահովման մոդելներից համացանցին ձեռք է բերել հաստատուն արագություն վերջին 10 տարիների ընթացքում: Ամպային տեխնոլոգիաները կամ ամպային համակարգչային գործողությունները (Cloud computing) տեղեկատվական տեխնոլոգիաների ծառայությունների մատուցման նոր մոդելներ են, որոնք համացանցի միջոցով տրամադրում են դինամիկ, մասշտաբային և հաճախ վիրտուալ ռեսուրսներ: «Ամպ» տերմինը բնորոշում է բարդ ենթակառուցվածքների կերպարը, որը քողարկում է բոլոր տեխնիկական մանրամասնությունները: Այդ դեպքում տեղեկատվությունը մշտապես պահպանվում է համաշխարհային ցանցի սերվերներում և ժամանակավորապես՝ հաճախորդի համակարգչում:

Խնդրի դրվածքը և մեթոդիկայի հիմնավորումը: Ցանկացած տեղեկատվության համար անհրաժեշտ է կիրառել պաշտպանության միջոցառումներ [2]: Դրանցից մեկը երկու սերվերի օգտագործումն է (այս տարբերակի ճիշտ կիրառումն ամենաապահով տարբերակներից է), որոնցից մեկը միացված է արտաքին ցանցին (1-ին սերվեր կամ վեբ սերվեր), իսկ 2-րդը (լուկալ սերվեր), այդ թվում՝ նաև տվյալների կենտրոնը, ներքին ցանցի միջոցով միացված է արտաքին սերվերներին կամ 1-ին սերվերին (նկ. 1): Այս դեպքում 2-րդ սերվերի տեղեկատվությունը գրեթե լիարժեք պաշտպանված է, և ամբողջ տեղեկատվությունը պահպանվում է 2 սերվերում:



Նկ. 1. Տեղեկատվության պաշտպանության հուսալի միջոցը

Ինչպես երևում նկ. 1-ից, արդյունքում ստացվում է 3 կապ: Օգտագործող - վեբ սերվեր - տվյալների կենտրոն:

Անհրաժեշտ է ապահովել անվտանգ կապն օգտատիրոջից դեպի վեբ սերվեր, քանի որ այդտեղ օգտագործվում է HTTP կապը կամ, այսպես կոչված, բաց ինտերնետային կապը: Ինչպես գիտենք, ինտերնետի ցանցային կապի վրա հարձակումները շատ ավելի հեշտ ու վտանգավոր են: Հաջորդ կարևոր խնդիրը

կլիենտի անձնական տվյալների, ինչպես նաև տվյալների բազայի անվտանգությունն ապահովելն է:

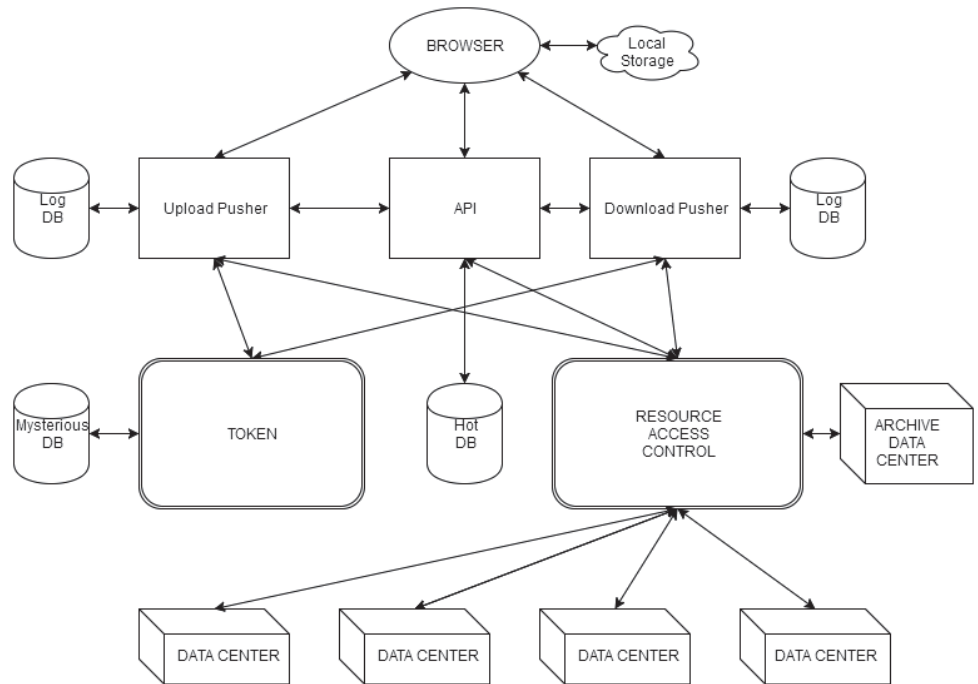
Աշխատանքում օգտագործվել են հարցումների կարգավորիչ (Load Balancer), վեբ սերվերներ, որոնք ապահովում են տվյալների «առաքումը» դեպի օգտվողի բրաուզեր, տվյալների կենտրոն, գաղտնագրված տվյալների բազաներ: Վեբ սերվերը կապվում է գաղտնի և գաղտնագրված տվյալների կենտրոնի հետ հատուկ մշակված արհեստական բանականության շերտի միջոցով, որն էլ իր հերթին ամպային տեխնոլոգիայի հիմնական շարժիչ ուժն է:

Հետազոտության արդյունքները: Առաջարկվող տարբերակում արտաքին սերվերները 3-ն են: Առաջինը նախագծված է որպես API (Application Program Interface) և նախատեսված է համակարգի աշխատանքը կազմակերպելու նպատակով: Այն պատասխանատու է վեբ կայքի էջերի և դրանց կառուցվածքի, սմարթֆոնային կամ համակարգչային ծրագրերի աշխատանքի և դրանց մեջ գտնվող տեղեկատվության, տեքստերի և նկարների ցուցադրման համար: Այս սերվերն ունի իր գաղտնագրված բազան: 2-րդ և 3-րդ արտաքին սերվերները նախատեսված են ֆայլերի տեղափոխման և դրա վրա ծախսվող ժամանակը զգալիորեն կրճատելու համար: Այս 2 սերվերները պատասխանատու են նաև բոլոր պլատֆորմներում ֆայլերի տեղափոխման և սինքրոնիզացման համար: Առաջին pusher-ը ապահովում է ֆայլերի ներբեռնումը օգտատիրոջ սարքավորումում: Հետևաբար՝ երկրորդն ապահովում է օգտատիրոջ համակարգչից վերբեռնումը դեպի սերվեր: Այս 3 սերվերները միասին սպասարկում են նաև այլ պլատֆորմների և միջավայրերի աշխատանքը, ինչպիսիք են՝ Windows, Linux, Android, iOS, Third-Party API's և այլն:

Ներքին սերվերները 2-ն են: Այս երկու սերվերները համակարգում են բոլոր գործողությունները: Առաջինն աշխատում է միայն կողմնորոշիչներով (token): Ամբողջ ամպային համակարգում ցանկացած ֆայլ, օգտատեր, տեղեկատվություն և գործողություն ունեն իրենց յուրահատուկ կոդերը, որոնք կոչվում են կողմնորոշիչներ: Դրանք սպասարկում են այն բոլոր սերվերների հարցումները, որոնք ունեն կողմնորոշիչների ստուգման, տեղադրելու կամ ստանալու կարիք: Ընդհանուր առմամբ՝ թղթենը օբյեկտ է, որը նկարագրում է մեկ այլ օբյեկտ: Եվ, վերջապես, 5-րդ սերվերը կոչվում է ռեսուրսների ղեկավարման սերվեր (Resource access control): Այն աշխատում է բացառապես ֆայլերի հետ: Ամբողջ ամպային համակարգում ֆայլերին դիմելու համար անհրաժեշտ է ստանալ այս սերվերի թույլտվությունը, և գործողություններ անում է միայն այս սերվերը: Այստեղ գործում է հակավիրուսային համակարգ, որն ունի բաց նախնական կոդ և կոչվում է ClamavNet: Մինչև տվյալների կենտրոն հասնելը նախ՝ ստուգվում է հակավիրու-

սով: Սերվերն ուղարկում կամ ստանում է ֆայլեր, կատարում փոփոխություններ: Այս սերվերն ունի իրեն հատկացված և մնացածից առանձնացված տվյալների կենտրոն, որը կոչվում է արխիվների կենտրոն: Երբ օգտագործողը ցանկանում է ներբեռնել ինչ-որ ֆայլ, այս սերվերը գտնում է համապատասխան ֆայլերը տվյալների կենտրոնից, ապա արխիվացնում և տեղափոխում է արխիվների սերվեր, որպեսզի ռեսուրսի տրամադրումն օգտատերերին կատարվի անհամեմատ ավելի արագ և առանց բրաուզերի կողմից խոչընդոտների: Նշենք, որ տվյալների կենտրոնը նույնպես գտնվում է ներքին միջավայրում և գլոբալ ցանցից չի ենթարկվում որևէ ազդեցության: Ցանկացած վեբ-կայքի հատկացվում է որոշակի հիշողություն զննարկիչում: Այնտեղ է պահվում ժամանակավոր կողմնորոշիչը, որով սերվերը ճանաչում է օգտագործողներին:

Նկ. 2-ում պատկերված է առաջարկվող ամպային համակարգի համառոտ գծագիրը, որտեղ երևում են սերվերները՝ ըստ իրենց անվանումների, և դրանց միջև կապը:



Նկ. 2. Ամպային համակարգի կառուցվածքը

Ցանցային կապի համար օգտագործվել են HTTPS (The Hypertext Transfer Protocol over SSL) և WSS (WebSocket over SSL) արձանագրությունները: Այս 2 արձանագրությունների անվտանգության համար օգտագործվել է SSL գաղտնա-

գրային արձանագրություն: Այն հնարավորություն է տալիս անվտանգ կապ հաստատել օգտվողի և սերվերի միջև: Տվյալ արձանագրությունն ապահովում է գաղտնիությունը՝ օգտագործելով TCP/IP, իսկ գաղտնագրման համար օգտագործելով բաց բանալիով ասիմետրիկ ալգորիթմ: Բաց բանալիով գաղտնագրման ժամանակ օգտագործվում է երկու բանալի, ըստ որում, դրանցից յուրաքանչյուրը կարող է օգտագործվել հաղորդագրության գաղտնագրման համար: Այնուամենայնիվ, եթե գաղտնագրման համար օգտագործվում է միայն մեկ բանալի, ապա վերջինս համար համապատասխանաբար պետք է օգտագործել մյուս բանալին: Այդ դեպքում կարելի է ընդունել պաշտպանված հաղորդագրություններ՝ հայտարարելով բաց բանալին, սակայն գաղտնի բանալին պահելով գաղտնի:

Առաջարկված ամպային համակարգում առանձնացնենք հետևյալ առանձնահատկությունները.

- Համակարգն ունի աշխատանքի արագության մեծ առավելություն մյուս համակարգերի նկատմամբ: Ըստ նախնական արդյունքների՝ գերազանցում է 1.2 անգամ:
- Ամպային կիրառական ծրագրերը ճկուն են և կարող են ավելանալ, պակասել և փոփոխվել հաշված վայրկյանների ընթացքում:
- Պլատֆորմը կարող է մատուցվել ինչպես ամպային, այնպես էլ ներքին ամպային ծրագրի տեսքով, որը ևս դրական ազդեցություն է ունենում ամպային տեխնոլոգիայի վրա:
- Ամպային համակարգը բավարարում է բիզնեսը բիզնեսին (B2B) և բիզնեսը հաճախորդին (B2C) պայմանները լիարժեք կերպով:

Այսպիսով, առաջարկված ամպային տեխնոլոգիան լիարժեք պաշտպանված է, պատրաստ՝ կիրառվելու գործնական խնդիրների լուծման համար:

Մշակված է համապատասխան ծրագրային միջոց, որի ամպային համակարգի ցանցային մուտքի հատվածքում աշխատում է ստեղծված overlord կոչվող հավելվածը: Այն տարբերակում է իրական հարցումները կեղծ հարցումներից: Կարողանում է տարբերակել DDOS հարձակումները և նույնիսկ DDOS հարձակման տեսակը (HTTP flood, ping flood, ICMP flood, UDP flood, SYN flood): Overlord-ով DDOS հայտնաբերման դեպքում ակտիվանում է overlord-ի antiddos կարգավորիչը, և ավտոմատ կերպով պատասխան հարձակում է իրականացվում հարձակվող սերվերի վրա, այս կերպ փորձելով լռեցնել հանցագործին: Իհարկե, սա չի օգնի մասշտաբային հարձակման դեպքում, այնուամենայնիվ, անվտանգության ապահովման ևս մեկ գործիք է, որը նպատակահարմար է կիրառման համար:

Մշակված համակարգն իր կառուցվածքով որոշ չափով պաշտպանված է սոցիալական ինժեներիայից: Այստեղ չեն պահպանվում օգտագործողի անձնական տվյալները, բացառությամբ նրա էլեկտրոնային փոստի հասցեից և անուն ազգանունից: Սոցիալական ինժեներիայով զբաղվողների օգուտը տեսականորեն շատ քիչ է սույն համակարգից: Այնուամենայնիվ, սոցիալական ինժեներիայից պաշտպանության համար գործում է գործոնային 2 վավերացում (2 factor authentication):

Առաջարկություն և եզրակացություն: Ամպային համակարգի բոլոր արտաքին սերվերները սպասարկում են բացառապես HTTP POST հրամաններ: Հարկավոր է պաշտպանվել անցանկալի POST հրամաններից: Ցանկացած սարքավորում, պլատֆորմ, որը կուղարկի ստանդարտներին չհամապատասխանող հարցումներ, անմիջապես արգելափակվում է: Արգելափակումը վերականգնելու համար պետք է դիմել անվտանգության և սպասարկման բաժին:

Մշակված համակարգում օգտագործված են 3 սերվերներ մուտք/ելքի ապահովման և 2 սերվերներ տվյալների պահպանման համար: Տվյալների փոխանցման անվտանգությունն ապահովվում է մշակված ծրագրային միջոցի կիրառմամբ:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Гатчин Ю.А., Климова Е.В.** Основы информационной безопасности: Учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.
2. **Меленец А.В.** Архитектура интеграции облаков распределенной системы хранения, оперативного обновления и предоставления данных о потенциально опасных объектах на основе технологии Cloud computing // Радиоэлектронні і комп'ютерні системи. - 2012. - № 7. -С. 54–59.

Կ.Գ. ՄԿՐՏՉԻԱՆ, Մ.Ա. ՆԱԼԲԱՆԴԻԱՆ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ

Изучены облачные технологии, их особенности, структура и дальнейшее развитие программного обеспечения. Основная задача состоит в том, чтобы обеспечить систему безопасности, конфиденциальность личной информации пользователей, доступность и т.д. Предложено оптимальное решение для обеспечения информационной безопасности.

Ключевые слова: облака, облачная технология, шифрование, безопасность.

K.G. MKRTCHYAN, M.A. NALBANDYAN

SECURITY IN CLOUD TECHNOLOGIES

Cloud technologies, their features, structure, software and future development have been studied. The main problem is securing the system, the user data privacy, availability, etc. An optimal solution has been proposed for the system information security.

Keywords: cloud, cloud technology, encryption, security.

УДК 621.373.826

А.А. СААКЯН

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ВОЛОКОННЫХ ЛАЗЕРОВ В СИСТЕМАХ ОПТИЧЕСКОЙ СВЯЗИ

Проведен анализ целесообразности применения волоконных лазеров в системах оптической связи. Обоснована необходимость детального электродинамического моделирования волоконных лазеров с зеркалами из волоконных брэгговских решеток с целью нахождения условий реализации одномодового режима работы лазера.

Ключевые слова: лазеры, волоконные лазеры, РОС-лазеры, РБО-лазеры, брэгговская решетка, волоконно-оптическая связь.

Лазеры, или оптические квантовые генераторы являются уникальными источниками когерентного излучения. Они нашли применение в военной технике, промышленности, медицине, системах навигации, связи и локации, химии, быту и т.д.

В современных системах волоконно-оптической связи широко используются полупроводниковые лазеры. Хотя они полностью обеспечивают потребности современной волоконно-оптической связи, однако их изготовление и стыковка с оптическим волокном представляют собой дорогостоящую процедуру.

В последние годы стремительное развитие получают волоконные лазеры, являющиеся сравнительно новыми устройствами квантовой электроники, которые создались на стыке лазерной физики и волоконной оптики. Эти лазеры обладают высоким качеством пучка, высокой эффективностью (~70%) и стабильностью генерации, высокой температурной и вибрационной стабильностью, надежностью и простотой эксплуатации, малыми размерами и весом. В волоконных лазерах не требуется юстировка зеркал, они являются перестраиваемыми и могут иметь многоволновую генерацию. В таких лазерах из-за волно-