L.G. KIRAKOSYAN

RESEARCH AND SELECTION OF OBJECT STORAGE SYSTEMS

Data management is the highest priority when distributing a cloud system. Storage should not only be reliable and secure, but also have the ability of scaling, while not causing problems with already established architecture. Big data storage, read/writing systems should be able to provide all the necessary tasks at high speeds without any interruptions. The document provides an analysis of storage systems for implementation in National Polytechnic University of Armenia cloud system.

***Keywords*:** data, data scaling, management, ceph, glusterfs, file system.

ՀՏԴ 004.22:004.421

Բ.Գ. ԱԹԱՅԱՆ

ՏՎՅԱԼՆԵՐԻ ԱՄՊԱՅԻՆ ՊԱՀՈՒՍՏԱՎՈՐՄԱՆ ՀԱՄԱԿԱՐԳՈՒՄ ՏԱՐԲԵՐԱԿՆԵՐԻ ԵՐԱՇԽԱՎՈՐՎԱԾ ՀԵՌԱՑՈՒՄԸ

Ներկայացվում է տվյալների պահուստավորման ամպային պաշտպանված համակարգ, որը գործում է որպես անվտանգության լրացուցիչ մակարդակ այսօրվա ամպային ծառայությունների օգտագործման պայմաններում: Տվյալների պահուստավորման ամպային համակարգում իրագործված է դրանց բազմակի պահուստավորման գործընացի լավարկման արդյունավետ վերապահուստավորման ալգորիթմ, որի օգտագործման շնորհիվ բացառվում է տվյալների պահուստների մի քանի տարբերակների ստեղծման արդյունքում առաջացած ավելցուկային տվյալների պահուստը համակարգում: Համակարգը ապահովում է նաև տվյալների պահուստների գաղտնագրային պաշտպանություն, մասնավորապես, պահուստների տարբեր տարբերակներում ընդգրկված տվյալների անվտանգ հեռացումը: Համակարգը հնարավորություն է տալիս օգտագործողներին հեռացնել պահուստների որոշակի տարբերակները և դարձնել դրանք անվերականգնելի, իսկ պահուստների այն տարբերակները, որոնք պարունակում էին ընդհանուր մասեր հեռացված տարբերակի հետ, կմնան հասանելի:

Առանցքային բառեր. ամպային պահուստավորում, երաշխավորված հեռացում, վերապահուստավորում, տարբերակների վերահսկում, բազմաշերտ գաղտնագրում:

Ամպային տեխնոլոգիաների զարգացման շնորհիվ ներկայումս այդ ոլորտում գործող ամպային ծառայությունները տրամադրում են հարմարավետ գործիքներ ֆիզիկական անձանց և կազմակերպություններին, ծախսելով քիչ գումարներ, պահպանել իրենց տվյալների պահուստային օրինակները ամպում: Սակայն ամպային ծառայության օգտագործողները պետք է ունենան ամպում պահվող տվյալների անվտանգության երաշխիքներ: Ամպում պահպանվող տվյալների անվտանգության ապահովման կարևորագույն խնդիր է երաշխավորված հեռա-

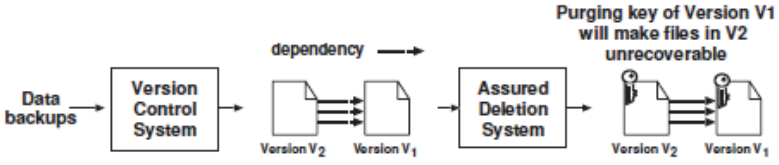
ցումը, այսինքն՝ օգտագործողի տվյալները ընդմիշտ անհասանելի դառնան ըստ հեռացման պահանջի: Պարզ է, որ պահուստային տվյալների ընդմիշտ պահպանումը ցանկալի չէ, քանի որ գաղտնի տեղեկատվությունը կարող է բացահայտվել, օրինակ՝ ամպային ծառայության օպերատորների սխալի, հաքերային հարձակման և այլ պատճառներով: Հավաստի հեռացումը տալիս է ամպային պահուստավորման համակարգի օգտագործողներին հնարավորություն՝ հուսալիորեն հեռացնելու իրենց պահուստային տվյալները՝ առանց վերականգնելու հնարավորության: Աշխատանքի նպատակն է ներդնել այդ հնարավորությունը ամպային պահուստավորման համակարգում, դարձնելով այն ավելի անվտանգ և, միևնույն ժամանակ, ապահովել օգտագործողների համար արդյունավետ միջոցներ՝ իրենց տվյալների պահուստների հետ աշխատելու համար:

Ամպային պահուստավորման համակարգում պահուստների տարբերակների վերահսկում: Համակարգի կարևորագույն մաս է կազմում տվյալների պահուստների տարբերակների վերահսկողության մոդուլը, որի միջոցով օգտագործողները կարող են իրենց տվյալները ետ վերադարձնել (rollback) տվյալի ավելի վաղ տարբերակին, այսինքն՝ չեղարկել ֆայլի վրա կատարված փոփոխությունները: Այս մոտեցումը առավել արդյունավետ է միևնույն տվյալների բազմակի վերապահուստավորման ժամանակ, երբ փոփոխված տարբերակը կցելով ավելի վաղ տարբերակին, հնարավոր է շահել թե՛ պահուստների պահպանման կրիչների օգտագործվող ծավալի մեջ, թե՛ պահուստավորման գործողության և ընտրված տարբերակի վերականգնման ժամանակի մեջ: Ամպային պահուստավորման համակարգում իրագործված է ինկրեմենտալ վերապահուստավորում, այսինքն, երբ պահուստի մեկ ինքնուրույն մասնիկը (ֆայլը) հայտվում է մի քանի տարբեր պահուստային օրինակների մեջ, իսկ մնացած տվյալները մնում են անփոփոխ, ապա վերապահուստավորվում է միայն փոփոխված ֆայլը, և ստեղծվում է պահուստի համապատասխան տարբերակ, որը պարունակում է տեղեկություն փոփոխված ֆայլի մասին: Մոտեցման գլխավոր թերությունն այն է, որ այս կերպ ստեղծվում են կախվածություններ պահուստային տարբերակների միջև, և, ընտրված տարբերակից ավելի վաղ տարբերակի վերացման արդյունքում ընտրված տարբերակը կարող է դառնալ անվերականգնելի: Տվյալ աշխատանքի նպատակն է լուծել նկարագրված խնդիրը և ներդնել համակարգում տարբերակների հավաստի հեռացման միջոցներ: Աշխատանքում ներկայացված տվյալների անվտանգ պահուստավորման ամպային համակարգը ապահովում է և՛ տարբերակների վերահսկողություն, և՛ դրանց հավաստի հեռացում, ընդ որում, ավելի վաղ տարբերակների հեռացման ժամանակ նոր տարբերակները կպահպանեն իրենց օգտագործելի վիճակը: Այս հնարավորությունը ապահովելու համար հա-

մակարգում օգտագործվում է բազմաշերտ գաղտնագրման մոտեցում, որը կնկարագրվի հաջորդ բաժնում:

Տվյալների պահուստների հավաստի հեռացում: Տվյալների հավաստի հեռացում ապահովելու համար ներկայումս նկարագրված է մի քանի եղանակ: Մեկ հնարավոր տարբերակն է անվտանգ վերագրումը (*secure overwriting)* [1], երբ ֆիզիկական կրիչի վրա նոր տվյալը գրվում է սկզբնական տվյալի տարածքում, ինչի արդյունքում վերջինս դառնում է անվերականգնելի: Սակայն, այսպիսի մոտեցումը ենթադրում է ֆայլային համակարգի փոփոխություններ, և, քանի որ պահուստի սերվերները սովորաբար սպասարկվում են երրորդ անձանց կողմից, ապա չկան երաշխիքներ, որ տվյալի ֆիզիկական տեղի վրա երբևիցե կարող է ուրիշ տվյալ գրվել: Մեկ այլ տարբերակ է տվյալի գաղտնագրումը պատահական բանալիով, ինչից հետո բանալին հեռացվում է, և տվյալը դառնում է անվերծանելի [2], [3], [4]: Սակայն նկարագրված մոտեցումները համատեղելի չեն ներկայումս օգտագործվող տարբերակների վերահսկման համակարգերին, քանի որ տարբերակների վերահսկման համակարգերը հիմնված են կրկնօրինակումից խուսափելու (deduplication) սկզբունքի վրա [5]:

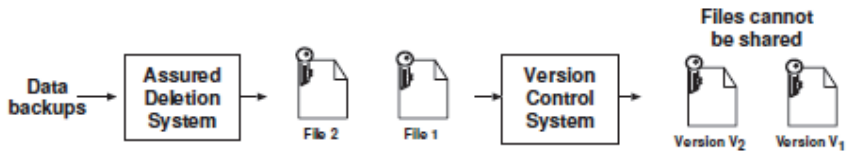
Ցուցադրելու համար տարբերակնեի վերահսկման համակարգերի և տվյալնեի հավաստի հեռացման մոտեցումների անհամատեղելիությունը, նկարագրենք այդ երկուսի օգտագործմամբ պահուստավորման երկու տարբեր ալգորիթմ: Առաջին տարբերակում սկզբում օգտագործում ենք պահուստների տարբերակների վերահսկման համակարգը, այնուհետև, անհրաժեշտության դեպքում, տվյալների հավաստի հեռացման համակարգը (նկ. 1): Ենթադրենք՝ սկզբում ստեղծվում է տարբերակ $V1$, այնուհետև տարբերակ $V2$:



Նկ. 1. Անհամատեղելիության ցուցադրման առաջին տարբերակը

Եթե երկու տարբերակում պարունակվում է նույն ֆայլի փոփոխություն, ապա կարելի է ասել, որ երկրորդ տարբերակը կախվածություն ունի առաջին տարբերակից: Արդյունքում հավաստի հեռացման համակարգը չի կարող լիարժեք գործել, քանի որ մեկ տարբերակի հեռացումը կհանգեցնի մյուսի անվերականգնելի վիճակին: Երկրորդ մոտեցման դեպքում սկզբում բոլոր պահուստները գաղտնագրվում են տարբեր բանալիներով (նկ. 2): Եթե երկու միանման ֆայլ գաղտնագրվում են տարբեր բանալիներով, ապա նրանց գաղտնագրված տար-

բերակները կտարբերվեն միմյանցից: Այս դեպքում տարբերակների վերահսկման համակարգը չի կարողանա հայտնաբերել, որ գաղտնագրված պահուստներում գտնվում է նույն ֆայլը, այսինքն՝ չի կարողանա գործել ինչպես նախատեսված է:

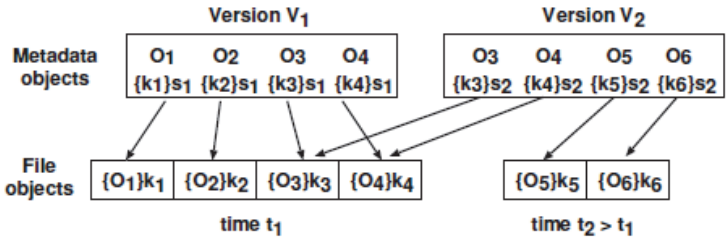


Նկ. 2. Անհամապատեղելիության ցուցադրման երկրորդ տարբերակը

Ամպային պահուստավորման համակարգում տարբերակների վերահսկման մոդուլի և հավաստի հեռացման մոդուլի համատեղելի աշխատանքի կազմակերպման համար իրագործված է երկմակարդակ գաղտնագրում, այսինքն, տարբերակների վերահսկման մոդուլին ավելացվում է գաղտնագրային պաշտպանության մի մակարդակ, որում տվյալները գաղտնագրվում են բանալիների առաջին մակարդակով (տվյալների բանալիներ), իսկ այդ բանալիները իրենց հերթին գաղտնագրվում են երկրորդ մակարդակի բանալիներով (կառավարող բանալիներ): Ենթադրենք՝ F ֆայլը հայտնվում է պահուստի մի քանի տարբերակներում: Սկզբում այն գաղտնագրվում է իր ուրույն k բանալիով, այնուհետև, այդ k բանալին իր հերթին գաղտնագրվում է տվյալ տարբերակի համար եզակի բանալիով: Նշանակենք P-ով դիմելու իրավունքի քաղաքականությունը O օբյեկտի համար, sP-ով՝ P-ի հետ կապված կառավարող բանալին, իսկ $\{O\}k$-ով՝ սիմետրիկ գաղտնագրման ալգորիթմով և k բանալիով՝ գաղտնագրված O օբյեկտը: Հետևաբար, որպեսզի կիրառենք $P_1, P_2, \cdots, և P_n$, քաղաքականությունները O օբյեկտի վրա, կատարվում է բազմաշերտ գաղտնագրում հետևյալ կերպ. $\{O\}k_{id}$, որտեղ k_{id} գաղտնագրվում է հետևյալ բանաձևով՝

$$\left\{\left\{\{k_{id}\}sP_1\right\}sP_2\cdots\right\}sP_n:$$

Եթե կառավարող sP_i $(1 \leq i \leq n)$ բանալիներից որևէ մեկը հեռացվում է, ապա k_{id} բանալին դառնում է անվերծանելի՝ O օբյեկտի հետ միասին: Այսպես, եթե հեռացնենք տարբերակը, այսինքն՝ տարբերակի եզակի բանալին, ապա հնարավոր չի լինի վերծանել այդ տարբերակում պահվող որևէ օբյեկտի բանալի, սակայն մյուս տարբերակներում հնարավոր կլինի վերծանել օբյեկտի բանալին՝ օգտագործելով տարբերակի բանալին (նկ. 3):



Նկ. 3. Երաշխավորված հեռացման և տարբերակների վերահսկման համատեղ կիրառումը

Որպեսզի վերականգնենք ֆայլը ընտրված տարբերակից, հարկավոր է սկզբում ստանալ տարբերակի եզակի բանալին, այնուհետև վերծանել այդ բանալիով ֆայլի բանալին և ստացված բանալիով վերծանել ֆայլը:

Տարբերակների և ֆայլերի բանալիների գեներացման համար համակարգում օգտագործվում է կեղծ պատահական թվերի գեներատոր: Այդ բանալիները գեներացվում են տարբերակի ստեղծման պահին և պահվում են ամպային համակարգում՝ բաշխված վիճակում: Որպես բանալիների բաշխման ալգորիթմ օգտագործվում է Շամիրի շեմային սխեման [6]:

Այսպիսով, տվյալների ամպային պահուստավորման համակարգում տվյալների անվտանգ վերապահուստավորման ներկայացված մեխանիզմը թույլ է տալիս միաժամանակ ունենալ պահուստների և տարբերակների վերահսկման մոդուլ, և տվյալների երաշխավորված հեռացման մոդուլ, ապահովում է դրանց համատեղ աշխատանքը: Համակարգում օգտագործվում է բազմաշերտ գաղտնագրման մեխանիզմ՝ պահուստների և տարբերակների բանալիների գաղտնագրման համար:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Gutmann P.** Secure deletion of data from magnetic and solid-state memory //Proc. of USENIX Security Symposium.- 1996.
2. **Boneh D. and Lipton R.** A Revocable Backup System //Proc. of USENIX Security Symposium.- 1996.
3. **Geambasu R., Kohno T., Levy A., and Levy H.** Vanish: Increasing data privacy with self-destructing data //Proc. of USENIX Security Symposium.- 2009.
4. **Perlman R.** File System Design with Assured Delete //ISOC NDSS.-2007.
5. **Anderson P. and Zhang L.** Fast and Secure Laptop Backups with Encrypted De-duplication //Proc. of USENIX LISA. - 2010.
6. **Shamir A.** How to Share a Secret //CACM. - Nov. 1979. - 22(11). – P.612–613.

Б.Г. АТАЯН

ГАРАНТИРОВАННОЕ УДАЛЕНИЕ ИНКРЕМЕНТАЛЬНЫХ РЕЗЕРВНЫХ КОПИЙ В ОБЛАЧНОЙ СИСТЕМЕ РЕЗЕРВНОГО ХРАНЕНИЯ

Разработан метод гарантированного удаления инкрементальных резервных копий в облачной системе резервного хранения. Предложенный метод предоставляет возможность основанному на понятии дедубликации механизму инкрементального резервного копирования и методу гарантированного удаления беспрепятственно работать вместе. Система облачного резервного копирования предоставляет средства гарантированного удаления из определенных версий резервных копий таким образом, чтобы не повлиять на работоспособность других версий. В системе используется многослойный метод шифрования путем введения различных ключей симметричного шифрования файлов и их соответствующих версий.

Ключевые слова: облачное резервное хранение, гарантированное удаление, инкрементальное резервное копирование, управление версиями, многослойное шифрование.

B.G. ATAYAN

ASSURED DELETION OF INCREMENTAL BACKUPS IN A CLOUD BACKUP SYSTEM

Assured deletion of incremental backup copies in cloud backup system is presented. The proposed method allows both the deduplication-based incremental backup mechanism and the assured deletion method to seamlessly work together. The cloud backup system provides means of assured backup deletion from particular backup versions in a way that will not affect other working backup versions. This functionality is achieved by using the layered encryption method by introducing different symmetric encryption keys for files and their corresponding versions.

Keywords*:* assured deletion, incremental backup, version control, cloud backup, layered encryption