MOBIL QURILMALARDAGI MA'LUMOTLARNI CLOUDDA XAVFSIZ SAQLASH ALGORITMI

Mualliflar

Odilbek Asqaraliyev

Perfekt Universiteti, Toshkent, O'zbekiston;

Samandar Yusupov

Kommunikatsiya va raqamli texnologiyalar kafedrasi, "University of management and future technologies" universiteti, Toshkent, 100208, O'zbekiston; samandar@umft.uz

Sirojiddin Xalilov

Kommunikatsiya va raqamli texnologiyalar kafedrasi, "University of management and future technologies" universiteti, Toshkent, 100208, O'zbekiston; khalilov@umft.uz

Mas'ul: khalilov@umft.uz

Annotatsiya: Ushbu ilmiy tadqiqot ishida axborotni kriptografik himoyalash tizimlari nazariyasi, ehtimollar nazariyasi, sonlar nazariyasi, matematik mantiq va kombinatorika metodlaridan foydalanilgan. Bulardan tashqari solishtirish, testlash va qiyosiy tahlil usullaridan foydalanildi. Mobil qurilamalardagi ma'lumotlarni xavfsizligini ta'minlash, Cloud Storageda ma'lumotlarni himoyalash va Cloud Storage texnologiyasida mavjud zaifliklarni bartaraf etishga qaratilgan xavfsizlik choralarini ishlab chiqish ishining nazariy ahamiyati sanaladi. Ma'lumotlarni himoyalashning mujassamlashgan usulidan foydalangan holda mobil qurilamalarda saqlanadigan va ishlanadigan axborotlarni Cloud Storage texnologiyasi asosida himoyalash samaradorligini oshirishga qaratilgan algoritmlar ishlab chiqildi.

Kalit so'zlar: Cloud computing, Cloud Storage, AES va SALSA20, SHA1 va MD5, shifrlash, Cloudda xavfsiz, Deshifrlash algoritmi.

ALGORITHM FOR SAFE STORAGE OF DATA ON MOBILE DEVICES IN THE CLOUD

Authors

Odilbek Asqaraliyev

Perfekt University, Tashkent, Uzbekistan;

Samandar Yusupov

Department of Communication and Digital Technologies, "University of Management and Future Technologies", Tashkent, 100208, Uzbekistan; samandar@umft.uz

Sirojiddin Khalilov

Department of Communication and Digital Technologies, "University of Management and Future Technologies", Tashkent, 100208, Uzbekistan; khalilov@umft.uz

Correspondence: khalilov@umft.uz

Abstract: The theory of cryptographic information protection systems, probability theory, number theory, mathematical logic and combinatorics methods were used in this research work. In addition, comparison, testing and comparative analysis methods were used. The theoretical importance of the development of security measures aimed at ensuring the security of data in mobile devices, protecting data in Cloud Storage and eliminating existing vulnerabilities in Cloud Storage technology is considered. Algorithms aimed at increasing the efficiency of protection of information stored and processed on mobile devices based on Cloud Storage technology using the integrated method of data protection were developed.

Keywords: Cloud computing, Cloud Storage, AES and SALSA20, SHA1 and MD5, Encryption, Secure in the Cloud, Decryption algorithm.

Kirish

Hozirgi kunda hayotimizni mobil qurilmalar, internet umuman olganda axborot texnologiyalarisiz tasavvur etish qiyin. Ular hayotimizning ajralmas qismiga aylanib ulgurdi. Ularning rivojlanishi natijasida ma'lumotlarimizni saqlash va ulardan foydalanish imkoniyatlari oshib bormoqda. Biz doimiy ravishda mobil qurilmalarimizda o'zimiz uchun kerakli bo'lgan axborotlarimi saqlaymiz, vaqti kelganida ularni kimgadir yuboramiz va kimdandir qabul qilib olamiz.

Bundan tashqari bulutli hisoblash texnologiyalari (Cloud computing) rivojlanishi natijasida biz o'z ma'lumotlarimizni bulutli serverlarda ya'ni Cloud Storagelarda [1] saqlash imkoniyatidan keng foydalanmoqdamiz.

Cloud computing elektron hisoblash xizmatlarini kompyuter tarmoqlari orqali yetkazib berishni nazarda tutadi va o'zida ma'lumotlarni saqlash tizimlari, turli ilovalar uchun platformalar, katta hisoblashlarni internet tarmog'ida mavjud kompyuterlardan foydalanib yechish kabi imkoniyatlarni yaratadi.

Bulutli texnologiyalar qulayliklar yaratish bilan bir qatorda muammolarni ham o'rtaga qo'ymoqda. Ushbu texnologiya mavjud imkoniyatlar bilan birgalikda Cloud Storageda saqlanayotgan ma'lumotlar xavfsizligini ta'minlash masalasini keltirib chiqarmoqda.

Materillar va usullar

Yuqorida aytib o'tilganidek, mobil qurilmalardagi ma'lumotlarni Cloudda xavfsiz saqlash dasturini ishlab chiqish uchun AES va SALSA20 shifrlash algoritmlari hamda SHA1 va MD5 heshlash funsiyalaridan foydalanilgan bo'lib, ulardan mujassamlashgan holda foydalanish orqali mobil qurilmalarda saqlanadigan va ishlanadigan axborotlarni Cloud Storage texnologiyasi asosida himoyalash samaradorligini oshirish mumkin. Mazkur mujassamlashgan usul orqali quyidagi muammolar hal etilgan:

- Foydalanuvchilarni autentifikatsiyalash;
- fayl nomi va mazmunini oshkor etmaslik;
- faylning kimga tegishli ekanligini yashirish;
- bir martalik kalitlardan foydalanish;
- ma'lumotlarni serverda shifrlangan ko'rinishda saqlash.

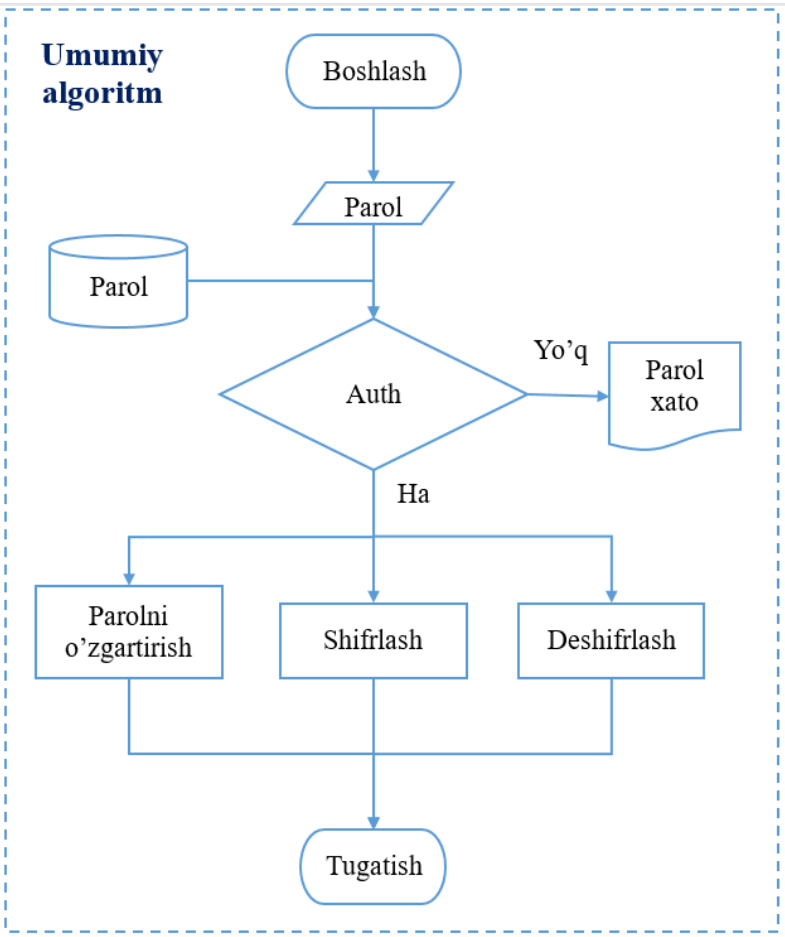
Foydalanuvchilarni autentifikatsiyalashda foydalanuvchining nomi mobil qurilmada ro'yhatdan o'tgan pochta manzili orqali unga ulanish paroli esa, shifrlash kalitidan foydalangan holda faylda saqlanadi. Ushbu parol joylashgan faylni ma'lumot tashuvchi qurilmada saqlash yoki bulutli serverlarda saqlash mumkin. Ushbu jarayonni amalga oshirish natijasida, klaviatura va qo'pol kuch hujumlaridan oldi olinadi[56].

Faylning kimga tegishli ekanligini yashirish. Ya'ni, faylning o'zi shifrlangan holda Cloudga yuboriladi. Foydalanuvchi emaillaridan esa xesh qiymati hisoblanib unga shifrlangan kalit qo'shiladi va u ham Cloudda saqlash uchun yuboriladi.

Hosil bo'lgan hesh qiymat tasodifiy belgilardan iborat bo'lib, u kimga tegishli ekanligini o'zida berkitib turadi.

Bir martalalik kalitlardan foydalanish. Bir martalik kalitlar har bir to‘plam nomi orqali yaratiladi. Ushbu kalit AES shifrlash algoritmi yordamida shifrlanadi va hosil bo‘lgan kalitni foydalanuvchi uchun tushunarli bo‘lgan joyda saqlab qo‘yiladi. Faylga har safar murojaat bo‘lganida ushbu fayl yangisiga o‘zgaradi. Ya’ni bir kalit faqat bir marta qo‘llaniladi.

Ma’lumotlarni serverda shifrlangan ko‘rinishda saqlashda SALSA algoritmidan foydalaniladi. Unda kalit sifatida yuqorida AES yordamida shifrlab faylda saqlangan tasodifiy, bir martalik kalit qo‘llaniladi.



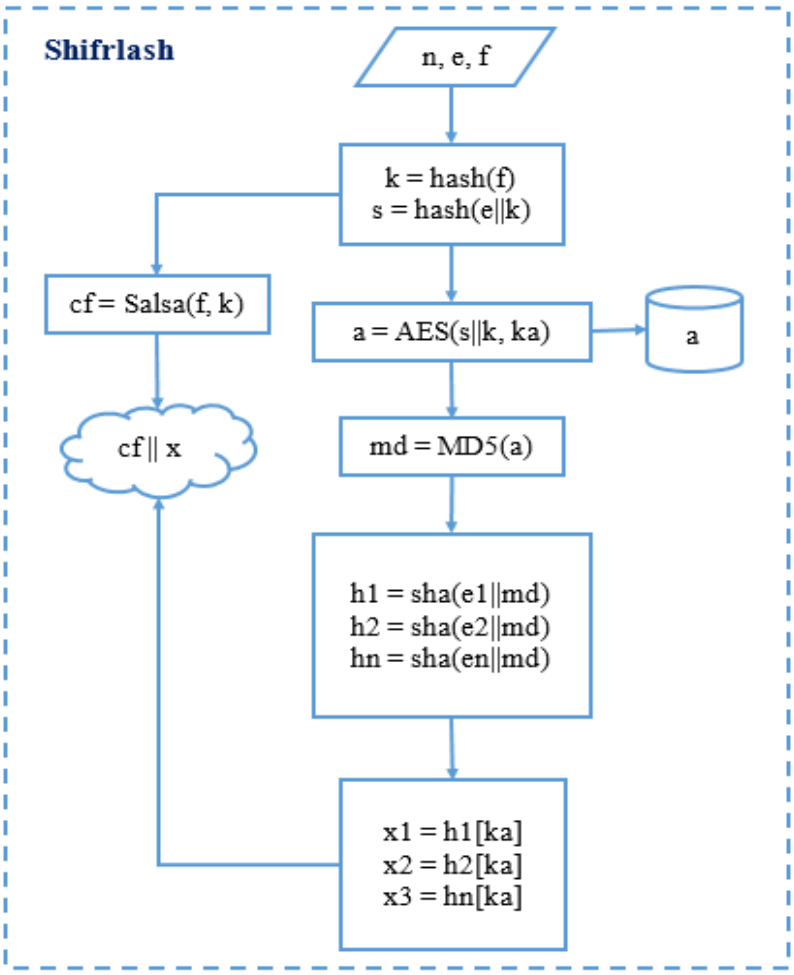
1-rasm. Dastur algoritmi.

Dasturga kirgandan so‘ng, dastlab foydalanuvchidan maxfiy parolni kiritish so‘raladi. Agar parol xato kiritilsa, dasturdan foydalanishga ruxsat berilmaydi.

Agar parol to‘g‘ri kiritilsa, dastur keying bosqichga o‘tadi. Unda quyidagilarni amalga oshirish mumkin:

- Maxfiy parolni o‘zgartirish;
- Ma’lumotlarni shifrlab Cloudga yuborish va deshifrlash uchun kerakli bo‘lgan qiymatlarni saqlab qo‘yish;
- Ma’lumotlarni Clouddan yuklab olish va ularni deshifrlab, foydalanuvchiga taqdim etish.

Shifrlash algoritmini ko‘radigan bo‘lsak, unda quyidagi ketma-ketliklar bajariladi:



2-rasm. Ma'lumotlarni shifrlab, Cloudga yuborish

Bunda, quyidagilarni izohlab o'tish zarur:

n – to'plam nomi;

e – foydalanish ruxsati berilgan electron pochtalar, ular bir nechta bo'lishi mumkin;

f – xavfsizligi ta'minlanishi kerak bo'lgan fayllar, ular shifrlanib, Cloud serverda saqlanadi;

Salsa – ma'lumotlarni shifrlash uchun ishlatiladigan algoritm, to'liq nomi Salsa20;

AES – shifrlashda ishlatilgan kalitni maxfiyligini ta'minlash uchun foydalaniladigan shifrlash algoritmi;

MD5, sha – xesh funksiyalar.

Dastlab kirish qiymati sifatida, to'plam nomi, foydalanish ruxsati berilishi kerak bo'lgan emaillar va konfidensialligi ta'minlanishi kerak bo'lgan fayllar tanlanadi.

So'ngra, belgilangan fayllar maxsus algoritm orqali shifrlanadi va belgilangan serverga yuboriladi. Shifrlashda ishlatilgan kalit esa, to'plam nomi bilan birgalikda AES shifrlash algoritmi orqali shifrlanadi.

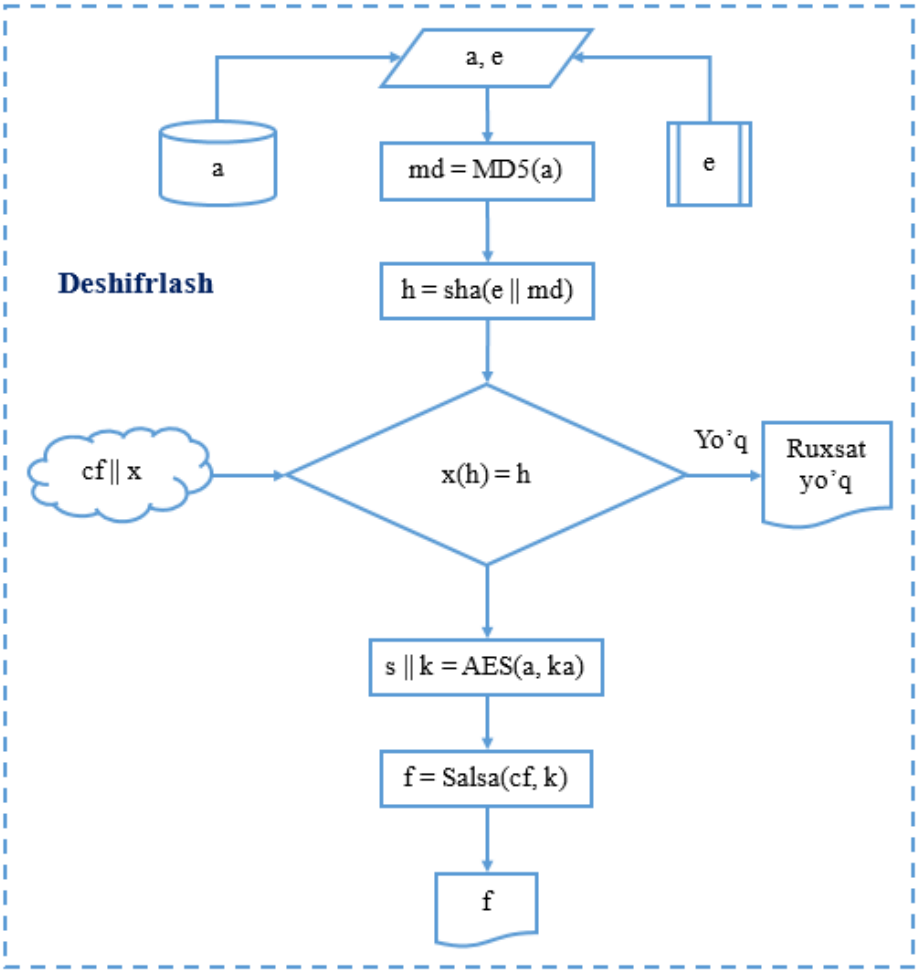
Keyin undan xesh qiymat olinib, ruxsat berilgan har bir emailga qo'shilgan holda yana bir bor xesh qiymatlar hosil qilinadi. Ushbu hech qiymatlarning har biriga, shifrlangan kalit biriktirilib, ular

ham belgilangan serverda saqlash uchun yuboriladi.

Keyingi algoritm Clouddan ma'lumotlarni yuklab olish va deshifrlab foydalanuvchiga taqdim etish bo'lib, 28-rasmda keltirilgan.

Aytish mumkinki bu bundan oldingi algoritmni aksi bo'lib, unda ham yuqorida keltirilgan shifrlaash algoritmlari va xeshlash funksiyalaridan foydalanilgan.

Shuni ta'kidlab o'tish lozimki, deshifrlash jarayonida hech qanday qiymat klaviatura orqali kiritlmaydi, ya'ni, algoritmda ko'rsatilgan akey va e qiymatlar mobil qurilmadan olinadi. Aniqroq qilib aytganda, akey shifrlash jarayonida mobil qurilmaga maxsus saqlab qo'yilgan kalit bo'lib, u mobil qurilma xotirasidan ko'rsatib qo'yiladi. E esa mobil qurilmada autentifikatsiyadan o'tgan electron pochta bo'lib, emailni kiritish paytida, mobil qurilmadagi electron pochtalar ro'yxati tqadim etiladi va ulardan birini tanlash so'raladi[55].



3-rasm. Deshifrlash algoritmi

Deshifrlash jarayoni qachonki foydalanuvchi o'zini haqiqiyligini tasdiqlagandagina amalga oshiriladi. Buning uchun, foydalanuvchi o'zining haqiqiyligini, unga foydalanish ruxsati berilganligini va unda maxsus kalit fayl mavjud ekanligini tasdiqlashi talab etiladi. Agar foydalanuvchi ularni to'g'ri taqdim eta olmasa, deshifrlash jarayoni amalga oshirilmaydi.

Xulosa

Tadqiqot ishida mobil qurilmalardagi ma'lumotlarni Cloudda xavfsiz saqlash dasturini ishlab chiqishga qaratilgan bo'lib, quyidagi natijalar olindi:

- Ma'lumotlarni Cloudda xavfsiz saqlash dasturida foydalanilgan shifrlash algoritmlari va xeshlash funksiyalari tadqiq etildi;
- Mazkur shifrlash algoritmlarining asosini tashkil etuvchi funksiyalar tadqiq etildi;
- Dastur algoritmi yaratildi;
- Yaratilgan algoritm asosida mobil qurilmalardagi ma'lumotlarni Cloudda xavfsiz saqlash dasturiy ta'minoti ishlab chiqildi;
- Dasturdan foydalanish imkoniyatlari batafsil keltirildi.

Adabiyotlar

1. Zhang, Yinghui, et al. "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing." Information Sciences 379 (2017): 42-61.
2. Aware, Preeti A., Vinayak Shinde, and Anand Aware. "Security Issues in Mobile Cloud Computing." Kaufman, Lori M. "Data security in the world of cloud computing." IEEE Security & Privacy 7.4 (2009).
3. Gupta, Shaurya, and Piyush Gupta. "A Study of the Issues and Security of Cloud Computing." International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5429-5434
4. Sarode, Rashmi P., Piyush Gupta, and Neeraj Manglani. "A comparative analysis of RSA and MD5 algorithms." Journal of Computer Science and Applications. ISSN (2014): 2231-1270.
5. Eswaraprasad, R., & Raja, L. (2017). A review of virtual machine (VM) resource scheduling algorithms in cloud computing environment. Journal of Statistics and Management Systems, 20(4), 703-711.
6. Suo, Hui, et al. "Security and privacy in mobile cloud computing." Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International. IEEE, 2013.