PAROLLAR ASOSIDA AUTENTIFIKATSIYALASH

Po’latov Doston Normurod o’g’li
Yoqubova Madinabonu Abdushukur qizi
Torebaeva Naziyra
Shonazarov Sarvarbek Maqsud o‘g‘li

Annotatsiya: *Autentifikatsiya tizimlari, foydalanuvchilarning kimlikni tasdiqlash va tizimga kirishni amalga oshirish uchun foydalaniladigan usullardir. Misollar shu usullardan ba'zi turlarini ko'rsatadi: parol autentifikatsiyasi, biometrik autentifikatsiya, birlashtirilgan autentifikatsiya usullari, yuborish kodlari va ikkinchi darajali autentifikatsiya. Bu usullar foydalanuvchilarga xavfsiz, ishonchli va moslashtirilgan autentifikatsiya tajribasini ta'minlashga yordam beradi. Har bir usulning o'zining afzalliklari va kamchiliklari mavjud bo'lib, foydalanuvchilarning xavfsizlik va foydalanishga qulay bo'lishini ta'minlash maqsadga muvofiq kerakli autentifikatsiya usulini tanlash juda muhimdir.*

Kalit so’zlar:*Autentifikatsiya, Identifikatsiya, Xavfsizlik, Maxfiylik,Xavfsiz parol,Qulay parol, Parol boshqarish tizimi, Parol yangilash,Xavfsizlik darajasi.*

Abstract: *Authentication systems are methods used to verify the identity of users and login to a system. Examples show some of these methods: password authentication, biometric authentication, combined authentication methods, submission codes, and second-level authentication. These methods help provide users with a secure, reliable, and personalized authentication experience. Each method has its own advantages and disadvantages, and it is important to choose the right authentication method in order to ensure security and ease of use for users.*

Keywords: *Authentication, Identification, Security, Privacy, Secure Password, Convenient Password, Password Management System, Password Update, Security Level.*

KIRISH

Parollar asosida autentifikatsiya, identifikatsiya va autentifikatsiya jarayonlarida foydalanuvchining kimligini tasdiqlashning eng ko'p ishlatiladigan usullardan biridir. Parol, foydalanuvchining yadrosi bo'lgan maxsus bir qator simvollardan iborat matndir.

Autentifikatsiya uchun parollarning bir nechta afzalliklari mavjud:

1. Xavfsizlik: Parollar foydalanuvchining kimligini himoya qilishda muhim ahamiyatga ega. Xavfsiz parollar, qo'lda bo'lmagan, to'g'ri formatga ega bo'lmagan, va bir nechta foydalanuvchi tomonidan ishlatilmaydigan matnlar bo'lishi kerak. Shuningdek, parollarning maxfiy saqlanishi va uzunligi ham xavfsizlikni ta'minlashda muhimdir.

2. Qulaylik: Foydalanuvchilar uchun parollar yodlanish va kiritishning qulay bo'lishi zarurdir. Parol kiritish jarayoni oson va foydalanuvchilar uchun yodlashi qulay bo'lishi kerak. Shuningdek, parollar uzunligi va kombinatsiyalari uchun qo'llanilgan belgilar to'plami ham qulaylikni oshiradi.

3. O'zgaruvchanlik: Parollarni boshqarish tizimi o'zgaruvchan parollar yaratishni ta'minlashi kerak. Foydalanuvchilar parollarini o'zgartirish, qayta tiklash va yangi parollar yaratish imkoniyatiga ega bo'lishi kerak. Bu, foydalanuvchilarning parollarini o'z vaqtida yangilab, xavfsizlik darajasi ni saqlashga imkon beradi.

4. Qo'llanish vaqtining minimal bo'lishi: Parollar uzun va xavfsiz bo'lishi kerak, lekin ulardan foydalanuvchilar uchun qo'llanish vaqtini ham tejam etmasligi kerak. Uzun, xavfsiz parollar foydalanuvchilar uchun yodlashni qiyinlashtirishi mumkin, shuning uchun parolni kiritish va autentifikatsiya jarayonlarida ishlatish vaqtini kamaytirishga intiladi.

Parollar, autentifikatsiya tizimlarining quyidagi afzalliklari bilan birgalikda kelajakdagi kiber xavfsizlikni ta'minlashda katta muhim ahamiyatga ega bo'ladi. Parollar foydalanuvchining kimligini tasdiqlash uchun o'ziga xos va muhim vositalardir.

Parollar asosida autentifikatsiyalashning bir qancha afzalliklari va kamchiliklari mavjud:

AFZALLIKLAR:

1. Osonlik: Parol asosida autentifikatsiya tizimi oson va foydalanuvchilar uchun yodlashi qulay bo'lishi mumkin. Parolni kiritish jarayoni oson va foydalanuvchilar tomonidan tez va osonlik bilan bajarilishi mumkin.

2. Kuzatuv: Parollar foydalanuvchining kimligini kuzatuv qilish uchun yaxshi bir vosita bo'lib xizmat qiladi. Xavfsiz parollar va yaxshi parol boshqarish tizimlari orqali parol so'rovlarini va kuzatuvni amalga oshirish mumkin.

3. Anonimlik: Parol asosida autentifikatsiya foydalanuvchining anonimligini ta'minlayadi. Parol orqali autentifikatsiya tizimiga kirish uchun foydalanuvchining haqiqiy kimligi va shaxsiy ma'lumotlarini ifshalamaydi.

KAMCHILIKLAR:

1. Xavfsizlik riski: Parol asosida autentifikatsiya tizimi xavfsizlik risklariga uchrayishi mumkin. Xavfsiz parol tanlash va parolni himoya qilish zarurati bor. Agar parol oqlash, qayta foydalanish yoki boshqa xavfsizlik muammo bo'lsa, foydalanuvchining kimligi va ma'lumotlari xavfsizlik xatariga duch kelishi mumkin.

2. Parolning unutish riski: Foydalanuvchilar parollarini unutish, yo'qotish yoki boshqalariga olib berish riski bor. Bu parol tiklash, yoritish so'rovlarini amalga oshirish va foydalanuvchining kirish ma'lumotlarini tiklash jarayonlarini murakkablashtirishi mumkin.

3. Qo'llash vaqti: Foydalanuvchilar uchun parolni kiritish va autentifikatsiya jarayonlari vaqt talab qiladi. Parolni to'g'ri kiriting, yangilash va qo'llab-quvvatlashga vaqt sarflanishi mumkin.

4. Parolni boshqarish muammosi: Foydalanuvchilar uchun ko'plab onlayn resurslarda turli parollar va parol politikalari bo'lishi mumkin. Bu, parollarni yodlash, o'zgartirish, qayta tiklash va saqlashning murakkab bo'lishi mumkin, shuning uchun foydalanuvchilar uchun boshqarish muammosi paydo bo'ladi.

Parollar asosida autentifikatsiyalashning afzalliklari va kamchiliklari, foydalanuvchining kimligini himoya qilish va tizimni foydalanuvchilar uchun oson va

mukammal bir autentifikatsiya tizimi tashkil etish imkonini beradi. Uning afzalliklari foydalanuvchilar uchun tez va oson autentifikatsiya, anonimlik va kuzatuv imkoniyatini ta'minlashdir. Kamchiliklar esa xavfsizlik risklari, parolning unutish riski va qo'llash vaqti kabi muammo va talablar bilan bog'liq bo'lishi mumkin.

Bundan tashqari, parollar asosida autentifikatsiya tizimlarida foydalanuvchilar tomonidan amalga oshiriladigan parolni yaxshi tanlash, xavfsiz saqlash va qo'llab-quvvatlash kerak. Qo'llanish vaqti jiddiy muhimiyatga ega bo'lib, foydalanuvchilar parollarini boshqarish va tiklash jarayonlariga ehtiyotkorlik bilan munosabat qilishi zarurati bor.

Parollarni yanada mustahkamlash uchun, ikki faktorli autentifikatsiya va biometrik ma'lumotlar (qo'l izi, yuz tanishligi kabi) kabi qo'shimcha tamoyillardan foydalanish mumkin. Bu usullar parollar asosida autentifikatsiyani yana ham etkazib berish va xavfsizlik darajasini oshirishga yordam beradi.

Asosiy qoida shundaki, foydalanuvchilar parollarini xavfsiz saqlash va yangilashga e'tibor berishlari, tizim administratorlarining esa xavfsizlikni ta'minlash uchun parol politikasini amalga oshirishlari va xavfsizlikni yuqori darajada saqlashlari muhimdir.

Asosiy qoida shundaki, parollar asosida autentifikatsiya tizimlari bir nechta afzalliklarga ega bo'lib, foydalanuvchilar uchun xavfsizlik va foydalanishni osonlashtiradi. Ular anonimlikni ta'minlayadi, kuzatuvni amalga oshiradi va foydalanuvchilar uchun osonlik va qulaylik yaratadi.

Bundan tashqari, parollar asosida autentifikatsiya tizimlarining kamchiliklari ham mavjud. Ularning eng muhim kamchiliklari xavfsizlik riski va parolning unutish riski. Xavfsizlik riski, xavfsiz parollar tanlashi, parolni himoya qilish va parolni to'g'ri saqlashni talab qiladi. Parolning unutish riski esa foydalanuvchilar uchun o'zgarishi, yodlashi va tiklashi kuchayadi.

Shuningdek, parolni boshqarish muammosi ham kamchiliklardan biridir. Parol politikasi va parolni yangilash jarayonlari foydalanuvchilar uchun murakkab bo'lishi mumkin. Bu, parollar to'g'ri saqlanmaganida va foydalanuvchilarning parollarini boshqalari bilan ulashish imkoniyati bo'lganida xavfsizlik xatariga olib kelishi mumkin.

Bundan tashqari, parollarning foydalanish vaqti ham kamchilik bo'lishi mumkin. Foydalanuvchilar uchun parolni kiritish, yangilash va saqlash jarayonlari vaqt va energiya talab qiladi.

Parollar asosida autentifikatsiya tizimlari afzalliklari va kamchiliklari foydalanuvchilar va tizim administratorlari uchun muhimdir. Xavfsizlik risklarini minimallashtirish, foydalanuvchilar uchun osonlik va xavfsizlikni ta'minlash uchun qo'llanish vaqti va parolni boshqarishni ehtiyotkorlik bilan amalga oshirish, muvaffaqiyatli autentifikatsiya jarayonlari uchun muhimdir.

Shundan so'ng, parollarni yanada mustahkamlash uchun ikki faktorli autentifikatsiya (2FA) kabi qo'shimcha tamoyillardan foydalanish tavsiya etiladi. Bu usul parol bilan birga boshqa identifikatsiya ma'lumotlarini ham talab qiladi, masalan, SMS yoki e-mail orqali

jo'natilgan tekshiruv kodi. Bu ikki faktorli yakuniy avtorizatsiya foydalanuvchilar uchun yana yuqori darajada xavfsizlikni ta'minlaydi.

Shuningdek, biometrik ma'lumotlar (qo'l izi, yuz tanishligi, ovoz) ham parollar asosida autentifikatsiyani yanada mustahkamlash uchun o'zbek tizimlarda qo'llanilmoqda. Bu usul foydalanuvchi identifikatsiyasini shaxsiy ma'lumotlarga asoslab olib, xavfsizlikni oshirishga yordam beradi. Biometrik autentifikatsiya uchun foydalanuvchi tomonidan ma'lumotlarni tiklash va saqlash zarurati mavjudligini aytish kerak.

Asosiy qoida shundaki, foydalanuvchilar parollarini xavfsiz saqlash, parol politikasini amalga oshirish va qo'llanish vaqti uchun ehtiyotkorlik bilan munosabat qilish kerak. Tizim administratorlarining esa xavfsizlikni ta'minlash uchun parol politikasini amalga oshirish, parollarini xavfsiz saqlash, parolni yangilash talablari va tizimdagi xavfsizlik tamoyillariga muvofiqlikni ta'minlashi zarurati mavjud.

Parollar asosida autentifikatsiya tizimlari foydalanuvchilar uchun xavfsizlikni ta'minlashda kritik ahamiyatga ega. Shu sababli, foydalanuvchilar va tizim administratorlari parollar bilan bog'liq tushunchalar va ko'nikmalarga tushunish, parollarini muhofaza qilish va xavfsizlik tamoyillariga amal qilishga e'tibor berishlari muhimdir.

Parollar asosida autentifikatsiya tizimlari, foydalanuvchilar uchun xavfsizlik va identifikatsiya muammolarini hal qilishda asosiy ahamiyatga ega. Bu tizimlar foydalanuvchilarning to'g'ri shaxsiy ma'lumotlarga kirishini ta'minlash, tizimlarini xavfsizligini saqlash, so'rov yuborish va javob olish jarayonlarida kimlikni tasdiqlash imkoniyatini beradi.

Parollar asosida autentifikatsiya tizimlarining afzalliklari orasida quyidagilar kiritilishi mumkin:

1. Xavfsizlik: Parollar foydalanuvchining ma'lumotlariga hech kimga kirish imkonini beradigan bir necha belgilardan iborat bo'lishi bilan xavfsizlikni ta'minlayadi.

2. Osonlik: Parollar oson tarzda yodlanishi va kirish jarayonida foydalanuvchilar uchun qulaylik yaratishi kerak. Bular foydalanuvchilarning yodlashi oson, hatto xususiy jadvalida saqlash imkoniyatini berishi mumkin.

3. Xavfsizlik so'rovlari: Parollar asosida autentifikatsiya tizimlari foydalanuvchilarga parolga qo'shimcha xavfsizlik so'rovlari berish imkonini beradi, masalan, ikki faktorli autentifikatsiya jarayonida tekshiruv kodi orqali kimlikni tasdiqlash.

4. Parol boshqarish: Tizim administratorlari uchun parollar bilan bog'liq boshqarish imkoniyatlari ham muhimdir. Bu parol politikasini belgilash, parollarni saqlash, yangilash va boshqa boshqarish jarayonlarini osonlashtiradi.

Parollar asosida autentifikatsiya tizimlarining kamchiliklari esa quyidagilar bo'lishi mumkin:

1. Xavfsizlik risklari: Foydalanuvchilarning parollarni o'zgartirish va saqlashda davom etadigan xavfsizlik risklari mavjud. Agar parollar yomon yoki o'zgartirishga imkon bermaydigan o'zbek shaxslaridan iborat bo'lsa, tizimlar hujjatlar, ikkita faktorli autentifikatsiya va boshqa xavfsizlik tamoyillari bilan qo'llanish kerak.

2. Parol boshqarish muammolari: Parollarni tiklash, yangilash va boshqarish jarayonlari foydalanuvchilar uchun qiyinliklarga olib kelishi mumkin. Parolni unutish, boshqalarga olib kelish, ma'lumotlar bazasining xavfsizlik xatariga olib kelish kabi muammolarga sabab bo'lishi mumkin.

3. Parol kompleksligi: Foydalanuvchilarga qo'yiladigan parol talablari ham yuzaga keladigan muammolardan biri bo'lishi mumkin. Juda oson yodlanadigan parollar yoki juda murakkab parollar foydalanuvchilar uchun qiyinliklar tug'dirishi mumkin. Parol kompleksligini belgilash va foydalanuvchilarga yaxshi parol tarkibi va uzunligi haqida tushuntirish muhimdir.

4. Qo'llash va o'zgartirish keraklik: Parollar o'z vaqti o'tgan holda zobitli bo'lishi mumkin. Foydalanuvchilar tomonidan to'g'ri saqlanmaydigan, unutilib qolgan yoki eski parollar tizim uchun xavfsizlik xatariga aylantirish mumkin. Parollarni boshqarishning oson va samarali usullari tizimlar uchun zarurdir.

Quyidagi misollar autentifikatsiya tizimlarini yaxshi tushuntirish uchun foydalanish mumkin:

1. Parol autentifikatsiyasi: Foydalanuvchi tizimga kirish uchun foydalanuvchi nomi va parolni kiritadi. Misol uchun, bir banka onlayn bank hisobiga kirish uchun foydalanuvchi nomi va shaxsiy parolni kiritishi talab qilinadi.

2. Biometrik autentifikatsiya: Foydalanuvchi identifikatsiyani o'rganish uchun biometrik ma'lumotlardan foydalanadi, masalan, qo'l izi, yuz skani yoki qo'l ajralmasi. Misol uchun, mobil telefonning oqibatlarni boshqarish uchun, foydalanuvchining qo'l izi skaneridan foydalanish mumkin.

3. Barcha ikkala usulni birlashtirish: Autentifikatsiya tizimida parol bilan birga biometrik ma'lumotlardan foydalanish mumkin. Bunday tizimda foydalanuvchi nomi, parol va biometrik ma'lumotlar, masalan, yuz skani yoki qo'l izi kiritilishi talab qilinadi.

4. Yuborish kodlari: Foydalanuvchiga kirish uchun autentifikatsiya kodlari yuborilishi mumkin. Misol uchun, SMS yoki e-mail orqali autentifikatsiya kodlari yuborish.

5. Ikkinchi darajali autentifikatsiya: Foydalanuvchining ikkinchi qadamda identifikatsiya uchun qo'llaniladigan biror bir narsa, masalan, yuborish kodini kiriting yoki biometrik ma'lumotlarni tasdiqlash. Misol uchun, bir banka onlayn hisobga kirish uchun foydalanuvchi parolni kiritgandan so'ng, telefoniga yuborilgan autentifikatsiya kodini kiritishi talab qilinadi.

Bu misollar autentifikatsiya tizimlarini tushuntirish uchun yordam beradi va foydalanuvchilarni xavfsizlik va identifikatsiya orasida yaxshi yo'naltirishga imkon beradi. Har bir autentifikatsiya usuli o'z afzalliklarini va kamchiliklarini ta'qib qiladi, shuning uchun foydalanuvchilar uchun qulay va xavfsiz autentifikatsiya usullari tanlash juda muhimdir.

Xulosa: Parollar asosida autentifikatsiya tizimlari, xavfsizlik va identifikatsiya muammolarini hal qilishda muhim o'rin egallaydi. Bu tizimlar yaxshi parol politikasi, xavfsizlik tamoyillari va foydalanuvchilar uchun qulayliklar bilan birga foydalanuvchilarni xavfsizlikning o'rtasida to'g'ri samarali autentifikatsiyaga yo'naltirishga yordam beradi.

Autentifikatsiya tizimlari parollar asosida foydalanuvchilar uchun identifikatsiya va xavfsiz kirishni ta'minlashda kritik ahamiyatga ega. Bu tizimlar foydalanuvchilarning ma'lumotlarga xavfsiz kirishini, kimlikni tasdiqlash imkoniyatini va tizimlarini xavfsizligini saqlashda muhim rol o'ynaydi.

AFZALLIKLAR:

- Autentifikatsiya tizimlari foydalanuvchilar uchun xavfsizlikni ta'minlayadi, xavfsiz kirish imkoniyatini beradi.

- Foydalanuvchilar oson va qulay parollarni yodlash orqali tizimga kirish imkoniyatiga ega bo'ladi.

- Parollar boshqarish usullari, parol politikasi va xavfsizlik tamoyillari orqali parollarning nazorat qilinishi va boshqarilishi oson bo'ladi.

- Autentifikatsiya tizimlari o'zgaruvchanlik va tashqi hujumlar bilan muhofaza qilinadi, foydalanuvchilarning ma'lumotlarini himoya qiladi.

Kamchiliklar:

- Foydalanuvchilar parollarni unutishi, xavfsiz saqlashda muammo tug'dirishi mumkin.

- Parollar yomon tarkibda yoki oson boshqarilmaydigan holda yaratilishi bilan xavfsizlik xatariga olib kelishi mumkin.

- Autentifikatsiya tizimlari tashqi hujumlarga nisbatan xavfsizligi ta'minlash uchun yoritilmishi kerak.

- Foydalanuvchilar parollarni tez o'zgartirish, qayta ishlatish va qo'llash bilan bog'liq qiyinliklarni tushuntirishi mumkin.

Barcha bilan, autentifikatsiya tizimlari foydalanuvchilar uchun xavfsizlik va identifikatsiyani ta'minlashda muhim ahamiyatga ega. Ularning afzalliklari va kamchiliklari parol boshqarish, xavfsizlik tamoyillari, foydalanuvchilar uchun qulaylik va xavfsizlik risklarini qo'llab-quvvatlash bilan bog'liq. Yaxshi boshqarilgan autentifikatsiya tizimi foydalanuvchilarni xavfsizlik va identifikatsiya orasida to'g'ri yo'naltirishi va tizimlar uchun maxsus xavfsizlikning ta'minlashiga yordam beradi.

FOYDALANILAGAN ADABIYOTLAR:

1. «Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

2.«Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

3. «Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

4. С.В. Симонов. Анализ рисков в информацион нмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

5.S.S.Qosimov. Axborot texnologiyalari. 0‘quv qoMlanma. - T.: «Aloqachi», 2006.

6.S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.