

قفل های هوشمند

دنیای امروز، قفل های هوشمند به عنوان یکی از اصلی ترین تکنولوژی های کاربردی در حوزه امنیت شناخته می شوند. این قفل های عملکردی بر اساس تکنولوژی ویژه ای عمل می کنند و به کمک آموزش های لازم، کاربران می توانند به راحتی از آن ها استفاده کنند

Amirshayan JALILI

Shayan138190@gmail.com

09101943345



Logo
Name

1. معرفی قفل های هوشمند
 2. انواع قفل های هوشمند
 3. مزایای استفاده از قفل های هوشمند
 4. مشکلات امنیتی
 5. امنیت یا قابلیت ها؟
 6. تمام حالات قفل های هوشمند
 7. پیاده سازی حالات با پایتون
 8. ایده نو برای قفل های هوشمند
- “تکنولوژی تشخیص الگوی رفتاری: رویکرد جدیدی برای امنیت قفل های هوشمند”
 - پیاده سازی در پایتون
9. **percept-action** جدول
 10. پیشنهادها نصب و راه اندازی قفل های هوشمند
 11. مورد استفاده قفل هوشمند
 12. در نقاط قوت امنیت قفل های هوشمند
 13. قابلیت های اضافی قفل های هوشمند
 14. نکات مهم در خرید و استفاده از قفل های هوشمند
 15. **برترین قفل هوشمند بازار**
 16. معیارهای انتخاب قفل های هوشمند
 17. **6. محصول برتر بازار**
 18. قفل های هوشمند دسترسی به اینترنت
 19. قفل های هوشمند و امنیت
 20. **معنای اختصار PEAS**
 - مثال عملی از موارد استفاده در قفل های هوشمند
 21. در قفل های هوشمند جست و جوی نا آگاهانه در قفل های هوشمند
 22. مسایل ارضای محدودیت در قفل های هوشمند
 23. **عامل مبتنی بر حل مساله انواع مساله**
 24. فرموله سازی مساله
 25. انواع جستجوهای نا آگاهانه
 26. **تعریف مسایل ارضای محدودیت**
 - انواع مسایل ارضای محدودیت
 - جستجوی عقبگرد
 - بهبود جستجو

معرفی قفل های هوشمند

قفل های هوشمند بر اساس تکنولوژی بی سیم ارتباط برقرار می کنند. همچنین، برای اینکه کمترین خطر امنیتی وجود نداشته باشد، با برنامه ها و دستگاه های دیگری نیز ارتباط برقرار می کنند که از تأیید اطلاعات مثل نام کاربر و رمز پیشگیری می کند

قفل های الکترونیکی

خصوصیات این نوع از قفل ها همانند تکنولوژی نگهداری کلید عملکرد می کند و تردیدی نیست که این قفل ها امنیت بالاتری را نسبت به قفل های سنتی دارند. برای این نوع از قفل ها کاربر باید از طریق ارسال پیامک، یا از طریق بلوتوث و فراتر از آن، از طریق اینترنت اعتبار خود را تأیید کند

قفل های بدون کلید

این نوع از قفل ها با فرمان و کنترل های مربوط به صدا، اثر انگشت و تشخیص چهره کاربران عمل می کنند. دسترسی به این قفل ها به سادگی صورت می گیرد و دیگر نیازی به استفاده از کلید وجود ندارد

قفل های کاربردی

این نوع از قفل ها با استفاده از اسانسورها، درب های چرخشی و یک سری تجهیزات دیگر استفاده می شوند و امکان پیچیدگی در دسترسی به آن ها وجود دارد

فل های هوشمند، قفل هایی هستند که از فناوری های مدرن مانند بی سیم، بیومتریک و برنامه های تلفن همراه این قفل ها مزایای زیادی نسبت به قفل های سنتی دارند، از برای باز و بسته کردن درب ها استفاده می کنند

جمله:

قفل های هوشمند از فناوری های امنیتی پیشرفته ای مانند اثر انگشت، تشخیص چهره و رمز: امنیت بالاتر عبور استفاده می کنند که می توانند امنیت خانه یا محل کار شما را به میزان قابل توجهی افزایش دهند

قفل های هوشمند نیاز به استفاده از کلید را از بین می برند، بنابراین می توانید درب ها را با راحتی بیشتر استفاده از تلفن همراه، اثر انگشت یا سایر روش های بیومتریک باز کنید

قفل های هوشمند را می توان از راه دور با استفاده از تلفن همراه یا سایر دستگاه های: قابلیت کنترل از راه دور این ویژگی می تواند برای باز کردن درب ها برای مهمانان یا کنترل دسترسی به خانه یا محل. هوشمند کنترل کرد کار شما از راه دور مفید باشد

انواع قفل های هوشمند

قفل های هوشمند را می توان بر اساس نوع فناوری مورد استفاده برای باز و بسته کردن درب ها به دسته های زیر تقسیم کرد:

این قفل ها با استفاده از یک کد عددی برای باز و بسته کردن درب ها استفاده می کنند: قفل های کدی

برای باز و بسته کردن درب ها استفاده می کنند RFID این قفل ها با استفاده از یک کارت: قفل های کارتی

این قفل ها با استفاده از اثر انگشت کاربر برای باز و بسته کردن درب ها استفاده می کنند: قفل های اثر انگشتی

این قفل ها با استفاده از تشخیص چهره کاربر برای باز و بسته کردن درب ها استفاده: قفل های تشخیص چهره می کنند

انواع قفل های هوشمند

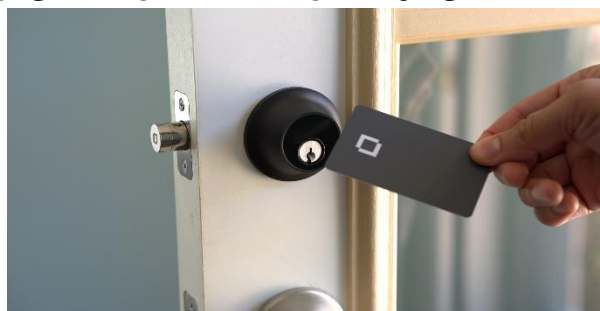
نوع مختلفی از قفل های هوشمند وجود دارد که هر کدام مزایا و معایب خاص خود را دارند. برخی از محبوب ترین انواع قفل های هوشمند عبارتند از:

این قفل ها با استفاده از یک کد عددی برای باز و بسته کردن درب ها استفاده می کنند. کدها معمولاً 4 تا 8 رقمی: قفل های کدی هستند و می توان آنها را به دلخواه تغییر داد. قفل های کدی نسبتاً ارزان هستند و نصب آنها آسان است. با این حال، آنها ممکن است ایمن ترین گزینه نباشند، زیرا کدها می توانند توسط افراد دیگر هک شوند.



قفل کدی هوشمند

برای باز و بسته کردن درب ها استفاده می کنند. کارت ها معمولاً حاوی RFID این قفل ها با استفاده از یک کارت: قفل های کارتی یک تراشه کوچک هستند که با قفل ارتباط برقرار می کند. قفل های کارتی ایمن تر از قفل های کدی هستند، زیرا کارت ها دشوارتر از کدها هک می شوند. با این حال، آنها ممکن است کمی گران تر از قفل های کدی باشند.



قفل کارتی هوشمند

این قفل ها با استفاده از اثر انگشت کاربر برای باز و بسته کردن درب ها استفاده می کنند. اثر انگشت ها: قفل های اثر انگشت منحصر به فرد هستند و بنابراین نسبتاً ایمن هستند. قفل های اثر انگشت راحت هستند، زیرا نیازی به حمل کارت یا وارد کردن کد ندارید. با این حال، آنها ممکن است کمی گران تر از قفل های کدی یا کارتی باشند.



قفل اثر انگشت هوشمند

این قفل ها با استفاده از تشخیص چهره کاربر برای باز و بسته کردن درب ها استفاده می کنند. قفل های تشخیص چهره تشخیص چهره می تواند ایمن تر از اثر انگشت باشد زیرا نمی توان آن را به راحتی با یک عکس جعلی کرد. قفل های تشخیص چهره راحت هستند، زیرا نیازی به حمل کارت یا وارد کردن کد ندارید. با این حال، آنها ممکن است گران ترین نوع قفل هوشمند باشند



قفل تشخیص چهره هوشمند

انتخاب نوع قفل هوشمند مناسب به عوامل مختلفی بستگی دارد، از جمله امنیت مورد نیاز شما، بودجه شما و راحتی مورد نظر شما

مزایای استفاده از قفل های هوشمند

امنیت و اعتماد

قفل های هوشمند بر پایه امنیت و کارایی بالا طراحی شده اند. معمولاً این قفل ها دارای قابلیت های ارتباطی گسترده ای هستند و با استفاده از آن ها امنیت بالاتری برای کاربر فراهم می شود.

سهولت در استفاده

با استفاده از قفل های هوشمند، کاربران نیازی به حفظ کلید و یادآوری رمزتان ندارند و فقط با استفاده از اثبات هویت می توانند به در دسترس خود دسترسی پیدا کنند.

راحتی در استفاده

این نوع قفل ها برای صاحبان خانه و دفتر کاری یک راه عملی و جذاب هستند.

قابلیت انعطاف پذیری

قفل های هوشمند در گروه تکنولوژی های جدیدی که قابلیت ارتباط سریع و پویا را دارند، قرار دارند و برای انواع مختلفی از استفاده مورد استفاده قرار می گیرند.

مشکلات امنیتی

آسان برداشته شدن

اکثر قفل های هوشمند به راحتی با دستگاه های خاص مانند هکرها قابل برداشت هستند.

مشکل در برقراری اتصال

در بعضی از مواقع، قفل های هوشمند نمی توانند به درستی به دستگاه های هوشمند متصل شوند و این مسئله می تواند باعث از دست رفتن امانت شما شود.

نحوه قفل کردن مشکوک است

برخی قفل های هوشمند با شکل و نحوه قفل کردن ظاهری مشکوک فارغ از کیفیت امنیتی بدسته های بزرگ سرای سرقت قرار می گیرند.

امنیت یا قابلیت ها؟

یکی از نقاط ضعف در سیستم امنیتی قفل های هوشمند، سوء استفاده از قابلیت های متنوع آن ها است؛ گاهی این قابلیت ها توجیهی برای کاستی در این سیستم هستند و بنابراین شکستی در مقابل حملات شبکه ای متقابل می باشند.

در شرایطی که همزمان با امنیت، قابلیت عملکرد نیز در کنار هم قرار داده شوند، باید به موازین قراردادن آن ها توجه کرد.

حالات قفل های هوشمند

توضیح	حالت قفل هوشمند
کاربر با استفاده از کلیدها، دکمه‌ها، اپلیکیشن موبایل یا روش‌های دیگر، قفل را باز یا بسته می‌کند.	باز و بسته کردن قفل
امکان کنترل قفل از محل دور با استفاده از اپلیکیشن موبایل یا ارتباطات بی‌سیم فراهم می‌شود.	کنترل از راه دور
قفل هوشمند دارای صفحه یا صفحه کلید برای وارد کردن کد عبور است که با وارد کردن کد، قفل باز می‌شود.	استفاده از کد عبور
برخی قفل‌های هوشمند از تکنولوژی تشخیص اثر انگشت برای شناسایی کاربر استفاده می‌کنند.	تشخیص اثر انگشت
برخی قفل‌های هوشمند از تکنولوژی تشخیص صدا برای شناسایی کاربر استفاده می‌کنند.	کنترل صدا
برخی قفل‌های هوشمند می‌توانند به شبکه بی‌سیم متصل شوند و از طریق اینترنت کاربر را مطلع کنند و قابلیت‌های دیگری را فراهم کنند.	اتصال به شبکه بی‌سیم
برخی قفل‌های هوشمند می‌توانند فعالیت‌های انجام شده را ضبط کنند و تاریخچه استفاده را نگهداری کنند.	ضبط فعالیت‌ها
برخی از قفل‌های هوشمند از تکنولوژی تشخیص چهره برای شناسایی کاربر استفاده می‌کنند.	تشخیص چهره
برخی از قفل‌های هوشمند از کارت‌های مغناطیسی یا RFID برای باز کردن قفل استفاده می‌کنند.	استفاده از کارت
برخی از قفل‌های هوشمند می‌توانند با استفاده از برچسب‌های NFC که به گوشی متصل شده‌اند، باز شوند.	استفاده از برچسب NFC
برخی از قفل‌های هوشمند می‌توانند با استفاده از بلوتوث گوشی کاربر، باز شوند.	استفاده از بلوتوث
برخی از قفل‌های هوشمند می‌توانند با استفاده از وای‌فای گوشی کاربر، باز شوند.	استفاده از وای‌فای
برخی از قفل‌های هوشمند می‌توانند با استفاده از اینفرارد گوشی کاربر، باز شوند.	استفاده از اینفرارد
برخی از قفل‌های هوشمند می‌توانند با استفاده از داده‌های بیومتریک کاربر، باز شوند.	استفاده از بیومتریک

پیاده سازی حالات در پایتون

```
class SmartLock:
    def __init__(self, password):
        self.locked = True
        self.password = password
        self.activity_log = []

    # باز و بسته کردن قفل
    def toggle_lock(self):
        self.locked = not self.locked
        self.log_activity('Lock toggled')
        return self.locked

    # کنترل از راه دور
    def remote_control(self, command):
        if command == 'UNLOCK':
            self.locked = False
            self.log_activity('Unlocked remotely')
        elif command == 'LOCK':
            self.locked = True
            self.log_activity('Locked remotely')
        return self.locked

    # استفاده از کد عبور
    def unlock_with_password(self, input_password):
        if input_password == self.password:
            self.locked = False
            self.log_activity('Unlocked with password')
            return self.locked

    # تشخیص اثر انگشت
    def unlock_with_fingerprint(self, input_fingerprint, actual_fingerprint):
        if input_fingerprint == actual_fingerprint:
            self.locked = False
            self.log_activity('Unlocked with fingerprint')
            return self.locked

    # کنترل صدا
    def unlock_with_voice(self, input_voice, actual_voice):
        if input_voice == actual_voice:
            self.locked = False
            self.log_activity('Unlocked with voice')
            return self.locked

    # اتصال به شبکه بی سیم
```

```
class AdvancedSmartLock:
    def __init__(self, password):
        self.locked = True
        self.password = password
        self.activity_log = []

    # باز و بسته کردن قفل
    def toggle_lock(self):
        self.locked = not self.locked
        self.log_activity('Lock toggled')
        return self.locked

    # کنترل از راه دور
    def remote_control(self, command):
        if command == 'UNLOCK':
            self.locked = False
            self.log_activity('Unlocked remotely')
        elif command == 'LOCK':
            self.locked = True
            self.log_activity('Locked remotely')
        return self.locked

    # استفاده از کد عبور
    def unlock_with_password(self, input_password):
        if input_password == self.password:
            self.locked = False
            self.log_activity('Unlocked with password')
            return self.locked

    # تشخیص اثر انگشت
    def unlock_with_fingerprint(self, input_fingerprint, actual_fingerprint):
        if input_fingerprint == actual_fingerprint:
            self.locked = False
            self.log_activity('Unlocked with fingerprint')
            return self.locked

    # کنترل صدا
    def unlock_with_voice(self, input_voice, actual_voice):
        if input_voice == actual_voice:
            self.locked = False
            self.log_activity('Unlocked with voice')
            return self.locked

    # اتصال به شبکه بی سیم
```



```
def connect_to_wifi(self, wifi_name):
    # این تابع باید با توجه به محیط خاص خود پیاده‌سازی شود
    pass

# ضبط فعالیت‌ها
def log_activity(self, activity):
    self.activity_log.append(activity)

# مشاهده فعالیت‌ها
def view_activities(self):
    return self.activity_log
```

```
def connect_to_wifi(self, wifi_name):
    # این تابع باید با توجه به محیط خاص خود پیاده‌سازی شود
    pass

# ضبط فعالیت‌ها
def log_activity(self, activity):
    self.activity_log.append(activity)

# مشاهده فعالیت‌ها
def view_activities(self):
    return self.activity_log
```

ایده نو برای قفل های هوشمند

“تکنولوژی تشخیص الگوی رفتاری: رویکرد جدیدی برای امنیت قفل‌های هوشمند”

بله، البته. تکنولوژی تشخیص الگوی رفتاری کاربر می‌تواند یک رویکرد جدید و جذاب برای امنیت قفل‌های هوشمند باشد. این تکنولوژی می‌تواند الگوهای رفتاری مانند سرعت و ریتم زدن کلید، فشار به کلید و حتی الگوی حرکت دست را یاد بگیرد و برای تشخیص هویت کاربر استفاده کند.

به عنوان مثال، فرض کنید که شما همیشه کلید را با یک سرعت خاص و با فشار خاصی می‌زنید، یا حتی وقتی که دست خود را به سمت قفل می‌برید، یک الگوی حرکت خاص دارید. این قفل هوشمند می‌تواند این الگوها را یاد بگیرد و در صورت تطابق با الگوی ذخیره شده، قفل را باز کند. این تکنولوژی می‌تواند یک لایه امنیتی اضافی را به قفل هوشمند اضافه کند.

این تکنولوژی می‌تواند به ویژه در محیط‌هایی که نیاز به امنیت بالا دارند، مانند سازمان‌ها و شرکت‌ها، مفید باشد. همچنین، با توجه به اینکه این تکنولوژی بر پایه رفتار کاربر است، احتمال دسترسی سایر افراد به سیستم کاهش می‌یابد، زیرا الگوی رفتاری هر فرد منحصر به فرد است.

با این حال، همچنین باید توجه داشت که این تکنولوژی ممکن است نیاز به زمان و منابع زیادی برای یادگیری و تطبیق دقیق الگوهای رفتاری داشته باشد. همچنین، ممکن است برخی از کاربران نگران حریم خصوصی خود باشند، زیرا این تکنولوژی می‌تواند الگوهای رفتاری آن‌ها را ثبت کند. بنابراین، هنگام استفاده از این تکنولوژی، باید به نگرانی‌های حریم خصوصی توجه شود.

در نهایت، استفاده از تکنولوژی تشخیص الگوی رفتاری کاربر می‌تواند یک راه جدید و جذاب برای افزایش امنیت قفل‌های هوشمند باشد، اما نیاز به تحقیقات بیشتری دارد تا بتواند به طور کامل و عملی پیاده‌سازی شود.

```
import time
```

```
class BehavioralSmartLock
```

```
    def __init__(self):
        self.locked = True
        self.press_times = []
```

```
    # باز و بسته کردن قفل
```

```
    def toggle_lock(self, press_time):
        self.press_times.append(press_time)
        if len(self.press_times) > 3:
            self.locked = not self.check_behavior()
        return self.locked
```

```
    # بررسی الگوی رفتاری
```

```
    def check_behavior(self):
        avg_time = sum(self.press_times) / len(self.press_times)
        return all(abs(t - avg_time) < 0.05 for t in self.press_times)
```

```
    # استفاده از قفل
```

```
lock = BehavioralSmartLock
```

```
start = time.time()
```

```
# فرض کنید کاربر کلید را فشار می‌دهد
```

```
lock.toggle_lock(time.time() - start)
```

```
start = time.time()
```

```
# فرض کنید کاربر دوباره کلید را فشار می‌دهد
```

```
lock.toggle_lock(time.time() - start)
```

```
start = time.time()
```

```
# فرض کنید کاربر سومین بار کلید را فشار می‌دهد
```

```
lock.toggle_lock(time.time() - start)
```

```
print(lock.locked) # اگر زمان فشار دادن کلید تقریباً یکسان بود، قفل باز می‌شود
```

```
python
import time

class BehavioralSmartLock:
    def __init__(self):
        self.locked = True
        self.press_times = []

    # باز و بسته کردن قفل
    def toggle_lock(self, press_time):
        self.press_times.append(press_time)
        if len(self.press_times) > 3:
            self.locked = not self.check_behavior()
        return self.locked

    # بررسی الگوی رفتاری
    def check_behavior(self):
        avg_time = sum(self.press_times) / len(self.press_times)
        return all(abs(t - avg_time) < 0.05 for t in self.press_times)

# استفاده از قفل
lock = BehavioralSmartLock()

start = time.time()
# فرض کنید کاربر کلید را فشار می‌دهد
lock.toggle_lock(time.time() - start)

start = time.time()
# فرض کنید کاربر دوباره کلید را فشار می‌دهد
lock.toggle_lock(time.time() - start)

start = time.time()
# فرض کنید کاربر سومین بار کلید را فشار می‌دهد
lock.toggle_lock(time.time() - start)

print(lock.locked) # اگر زمان فشار دادن کلید تقریباً یکسان بود، قفل باز می‌شود
```

Percept_action

Percept (ادراک)	Action (عمل)
کاربر کلید را فشار می‌دهد	قفل باز یا بسته می‌شود
دریافت دستور از راه دور	قفل باز یا بسته می‌شود
ورود کد عبور	قفل باز می‌شود اگر کد عبور صحیح باشد
تشخیص اثر انگشت	قفل باز می‌شود اگر اثر انگشت مطابقت داشته باشد
تشخیص صدا	قفل باز می‌شود اگر صدا مطابقت داشته باشد
اتصال به شبکه بی‌سیم	قفل اطلاعات را از طریق اینترنت ارسال می‌کند
ضبط فعالیت‌ها	قفل فعالیت‌های انجام شده را ضبط می‌کند
تشخیص چهره	قفل باز می‌شود اگر چهره مطابقت داشته باشد
استفاده از کارت	قفل باز می‌شود اگر کارت معتبر باشد
NFC استفاده از برچسب	معتبر باشد NFC قفل باز می‌شود اگر برچسب
استفاده از بلوتوث	قفل باز می‌شود اگر دستگاه بلوتوث معتبر باشد
استفاده از وای‌فای	قفل باز می‌شود اگر دستگاه وای‌فای معتبر باشد
استفاده از اینفرارد	قفل باز می‌شود اگر دستگاه اینفرارد معتبر باشد
استفاده از بیومتریک	قفل باز می‌شود اگر داده‌های بیومتریک مطابقت داشته باشد
تشخیص الگوی رفتاری	قفل باز می‌شود اگر الگوی رفتاری مطابقت داشته باشد

پیاده سازی در پایتون

```

class Door :
def __init__(self):
self.locked = True

def press_key(self):
self.locked = not self.locked

def remote_command(self, command):
if command == 'UNLOCK':
self.locked = False
elif command == 'LOCK':
self.locked = True

def enter_password(self, input_password, actual_password):
if input_password == actual_password:
self.locked = False

def fingerprint_detected(self, input_fingerprint, actual_fingerprint):
if input_fingerprint == actual_fingerprint:
self.locked = False

def voice_detected(self, input_voice, actual_voice):
if input_voice == actual_voice:
self.locked = False

def wifi_connected(self):
# This function needs to be implemented according to your specific environment
pass

def log_activity(self):
# This function needs to be implemented according to your specific environment
pass

def face_detected(self, input_face, actual_face):
if input_face == actual_face:
self.locked = False

def card_used(self, input_card, actual_card):
if input_card == actual_card:
self.locked = False

def nfc_tag_detected(self, input_nfc_tag, actual_nfc_tag):
if input_nfc_tag == actual_nfc_tag:
self.locked = False

def bluetooth_device_detected(self, input_device, actual_device):
if input_device == actual_device:
self.locked = False

def wifi_device_detected(self, input_device, actual_device):
if input_device == actual_device:
self.locked = False

def infrared_device_detected(self, input_device, actual_device):
if input_device == actual_device:
self.locked = False

def biometric_data_detected(self, input_data, actual_data):
if input_data == actual_data:
self.locked = False

def behavior_pattern_detected(self, input_pattern, actual_pattern):
if input_pattern == actual_pattern:
self.locked = False

```

پیشنهادهای

برای بهبود قفل های هوشمند، به چند مورد نیاز است

استفاده از نرم افزارهای پیشرفته

استفاده از نرم افزارهای جدیدتری که برای جلوگیری از هک شدن طراحی شده‌اند، به عنوان پدیده الکترونیکی محافظتی راه حلی قابل قبول است.

ارائه ارزیابی های امنیتی

مسئولین سازمان ها و شرکت ها باید در خصوص پیش آمدن حوادث امنیتی در قفل های هوشمند، ارزیابی های لازم ارائه دهند و راه حل بهبودی را بر اساس این نتایج، در نظر بگیرد.

استفاده از قفل های فیزیکی اضافی

در نهایت در صورت نیاز، می توانید به استفاده از قفل های فیزیکی اضافی، به عنوان یک اقدام پیش مانده، از احتمال سرقت و جرم در برابر شرکت خود جلوگیری کنید

نصب و راه اندازی قفل های هوشمند

نصب قفل الکترونیکی به سادگی در هرجایی انجام می شود.

نصب قفل های به شدت روی حریم خصوصی و امنیت حساب شما تأکید دارد.

آموزش های نصب و راه اندازی قفل های هوشمند و به عنوان مثال «هدایت الکترونیکی» با خدمات مشابه ارائه می شوند.

با این حال، مهم است که نصب قفل های هوشمند معمولاً آسان است و می توان آن را در عرض چند دقیقه انجام داد. دستورالعمل های نصب را به دقت دنبال کنید تا از نصب صحیح قفل اطمینان حاصل کنید.

مراحل نصب قفل هوشمند

قبل از شروع نصب، مطمئن شوید که موارد زیر را دارید. موارد مورد نیاز را آماده کنید

قفل هوشمند

باتری ها

پیچ گوشتی

مته

نوار اندازه گیری

مداد

این اندازه گیری ها را برای اطمینان با استفاده از نوار اندازه گیری، عرض و ارتفاع قاب درب را اندازه گیری کنید. اندازه گیری کنید از خرید قفل هوشمند مناسب با قاب درب خود استفاده کنید.

دستورالعمل های نصب را که همراه با قفل هوشمند شما ارائه شده است دنبال کنید تا قفل را روی قاب درب قفل را نصب کنید. معمولاً باید پیچ گوشتی یا مته برای نصب قفل استفاده کنید. نصب کنید.

معمولاً یک مکان مخصوص برای قرار دادن باتری ها در قفل وجود باتری ها را در داخل قفل قرار دهید. باتری ها را نصب کنید دارد.

این شامل افزودن کاربران، ایجاد رمزها و با استفاده از برنامه تلفن همراه یا رایانه، قفل را پیکربندی کنید. قفل را پیکربندی کنید. کارت ها و تنظیم سایر تنظیمات است.

راه اندازی قفل های هوشمند

این شامل افزودن کاربران، ایجاد رمزها و کارت ها و تنظیم سایر تنظیمات. پس از نصب قفل هوشمند، باید آن را راه اندازی کنید است.

مراحل راه اندازی قفل هوشمند

برنامه تلفن همراه یا رایانه ای که قفل هوشمند شما با آن سازگار است را دانلود کنید. برنامه تلفن همراه یا رایانه را دانلود کنید.

برای دسترسی به قفل هوشمند خود، باید یک حساب کاربری ایجاد کنید. برنامه را باز کنید و حساب کاربری ایجاد کنید.

دستورالعمل های برنامه را دنبال کنید تا قفل را به برنامه اضافه کنید. قفل را به برنامه اضافه کنید.

این می تواند شامل اعضای خانواده، دوستان، مستاجران و غیره باشد. کاربران را به قفل خود اضافه کنید. کاربران را اضافه کنید.

این رمزها و کارت ها به کاربران امکان می دهد تا رمزها و کارت ها را برای کاربران خود ایجاد کنید. رمزها و کارت ها را ایجاد کنید. قفل را باز کنند.

سایر تنظیمات را مانند روشن یا خاموش کردن آلارم و تنظیم اعلان ها را پیکربندی کنید. سایر تنظیمات را پیکربندی کنید.

نکات ایمنی برای قفل های هوشمند

با این حال، مهم است که نکات قفل های هوشمند می توانند امنیت خانه یا محل کار شما را به میزان قابل توجهی افزایش دهند.

ایمنی زیر را برای محافظت از قفل خود و اطلاعات شخصی خود دنبال کنید.

از رمزهای عبور قوی استفاده کنید که شامل حداقل 8 کاراکتر از حروف بزرگ، حروف کوچک، اعداد و نمادها باشند.
 رمزهای عبور خود را به طور منظم تغییر دهید تا از هک شدن آنها جلوگیری کنید. رمزهای عبور خود را به طور منظم تغییر دهید
 کارت ها و اثر انگشت های خود را ایمن نگه دارید تا دیگران نتوانند از آنها برای باز . کارت ها و اثر انگشت ها را ایمن نگه دارید
 کردن قفل شما استفاده کنند
 این به . سازنده قفل شما معمولاً به روزرسانی های نرم افزاری را برای قفل خود منتشر می کند . قفل خود را به روز نگه دارید
 روزرسانی ها می توانند شامل رفع اشکالات و بهبود امنیت باشند

مورد استفاده قفل هوشمند در نقاط قوت

قفل های هوشمند مزایای زیادی نسبت به قفل های سنتی دارند. برخی از نقاط قوت قفل های هوشمند عبارتند از:

- امنیت بیشتر: قفل های هوشمند از فناوری های امنیتی پیشرفته مانند اثر انگشت، تشخیص چهره یا رمزنگاری استفاده می کنند که می توانند امنیت خانه یا محل کار شما را به میزان قابل توجهی افزایش دهند.
- راحتی بیشتر: قفل های هوشمند نیاز به استفاده از کلید را از بین می برند، بنابراین می توانید درب ها را با استفاده از تلفن همراه، اثر انگشت یا سایر روش های بیومتریک باز کنید.
- قابلیت کنترل از راه دور: قفل های هوشمند را می توان از راه دور با استفاده از تلفن همراه یا سایر دستگاه های هوشمند کنترل کرد. این ویژگی می تواند برای باز کردن درب ها برای مهمانان یا کنترل دسترسی به خانه یا محل کار شما از راه دور مفید باشد.
- در اینجا چند مثال خاص از نحوه استفاده از نقاط قوت قفل های هوشمند آورده شده است:
- یک قفل هوشمند با فناوری اثر انگشت می تواند از خانه شما در برابر ورود غیرمجاز توسط سارقانی که کلید شما را ندارند محافظت کند.
- یک قفل هوشمند با برنامه تلفن همراه می تواند به شما امکان دهد درب را از راه دور باز کنید، حتی اگر در خانه نباشید.
- یک قفل هوشمند با کلیدهای دیجیتالی می تواند به شما امکان دهد به طور موقت به دیگران دسترسی به خانه یا محل کار خود بدهید.
- با توجه به این نقاط قوت، قفل های هوشمند می توانند گزینه ای عالی برای بهبود امنیت و راحتی خانه یا محل کار شما باشند.

امنیت قفل های هوشمند

قابل توجه تمامی کاربران: قفل های هوشمند با استفاده از رمزهای کاربر رمزگذاری شده به صورت امن و کدگذاری شده اعتبارشان را تأیید می کنند و به اینترنت، از طریق بلوتوث و مراکز مجاز دسترسی پیدا می کنند. لذا قوانین استفاده از رمز و عملکرد اصلی قوانین را به عهده می گیرد.

هکرها به طور پیوسته قفل های هوشمند را هدف قرار داده اند و برای آزمایش هوشمندی راه های زیادی برای خرید یک پردازنده الترا از پول فروشگاه بانکی یا سرویس امنیتی به منظور شکستن رمز های الکترونیکی ارائه کرده اند.

قفل های هوشمند معمولاً ایمن تر از قفل های سنتی هستند. آنها از فناوری های امنیتی پیشرفته ای مانند اثر انگشت، تشخیص چهره و رمز عبور استفاده می کنند که می توانند امنیت خانه یا محل کار شما را به میزان قابل توجهی افزایش دهند.

با این حال، مهم است که به یاد داشته باشید که هیچ قفل کاملاً ایمن نیست. قفل های هوشمند نیز می توانند هک شوند، بنابراین مهم است که نکات ایمنی را برای محافظت از قفل خود و اطلاعات شخصی خود دنبال کنید.

برخی از عواملی که می توانند بر امنیت قفل های هوشمند تأثیر بگذارند عبارتند از:

- نوع قفل: برخی از انواع قفل های هوشمند ایمن تر از سایرین هستند. به عنوان مثال، قفل های اثر انگشت معمولاً ایمن تر از قفل های کدی هستند.
- ویژگی های امنیتی: برخی از قفل های هوشمند از ویژگی های امنیتی اضافی مانند تأیید دو مرحله ای یا هشدارهای امنیتی برخوردار هستند که می توانند امنیت را افزایش دهند.
- به روزرسانی های نرم افزاری: سازنده قفل شما معمولاً به روزرسانی های نرم افزاری را برای قفل خود منتشر می کند. این به روزرسانی ها می توانند شامل رفع اشکالات و بهبود امنیت باشند.

در اینجا چند نکته برای افزایش امنیت قفل هوشمند خود آورده شده است:

- رمزهای عبور قوی استفاده کنید. از رمزهای عبور قوی استفاده کنید که شامل حداقل 8 کاراکتر از حروف بزرگ، حروف کوچک، اعداد و نمادها باشند.
 - رمزهای عبور خود را به طور منظم تغییر دهید. رمزهای عبور خود را به طور منظم تغییر دهید تا از هک شدن آنها جلوگیری کنید.
 - کارت ها و اثر انگشت ها را ایمن نگه دارید. کارت ها و اثر انگشت های خود را ایمن نگه دارید تا دیگران نتوانند از آنها برای باز کردن قفل شما استفاده کنند.
 - قفل خود را به روز نگه دارید. سازنده قفل شما معمولاً به روزرسانی های نرم افزاری را برای قفل خود منتشر می کند. این به روزرسانی ها می توانند شامل رفع اشکالات و بهبود امنیت باشند.
- با پیروی از این نکات ایمنی، می توانید از قفل هوشمند خود و اطلاعات شخصی خود محافظت کنید.

قابلیت های اضافی قفل های هوشمند

قفل های هوشمند برخلاف قفل های سنتی دارای قابلیت هایی هستند که برای بهبود کارآیی و کاربرد آنها، استفاده می شود. این قابلیت ها می توانند شامل مواردی مانند دیدن وضعیت اتاق یا اتاق خانه، کنترل نورپردازی، چراغ خاموش کردن، کنترل کنترل از راه دور و دیگر قابلیت ها باشند

همراهی با دوربین مدار بسته

با همراهی قفل های هوشمند با دوربین، می توان تصویر تمامی قطعات خانه در بخش لوح شود

وکی ۹۷ می شود Waze مسیر یابی داخلی که در آن در برنامه های مانند

مسیر یابی داخلی برای کاربران، به استفاده از قفل های هوشمند اجازه می دهد تا تنها با استفاده از یک قفل الکترونیکی، اتاق وارد را ببینند

GPS استفاده از موقعیت یاب داخلی و برنامه های

، می توان به یک محل خاص اشاره GPS قفل های هوشمند با استفاده از موقعیت یاب، به آدرس شناخته شده و آدرس از طریق کرد

نکات مهم در خرید و استفاده از قفل های هوشمند

بررسی پیشینه شرکت

پیش از خرید قفل هوشمند، بهتر است به بررسی پیشینه شرکت سازنده و محصولاتی که به همراه قفل هوشمند ارائه می دهد توجه داشته باشید

برنامه های امنیتی

، بهتر است با استفاده از برنامه های více با استفاده از زیرساخت های ارائه شده توسط قفل های هوشمند، پیش از خرید آن امنیتی اطمینان حاصل کنید قبل از استفاده در زمینه هایی مانند حفظ رویکرد قانونی و حریم خصوصی

تعویض کلیدها

قفل های هوشمند به خاطر تکنولوژی به کار رفته در کلید ها خصوصیات خود را دارند. چنین استفاده از قفل های هوشمند و عملکرد دقیق کلید برای قفل های هوشمند، رعایت دقیق تعویض کلید ها اهمیت دارد

نکات مهم در خرید قفل های هوشمند

قفل های هوشمند مزایای زیادی نسبت به قفل های سنتی دارند، اما قبل از خرید یک قفل هوشمند، مهم است که نکات زیر را در نظر بگیرید:

- نوع قفل: انواع مختلفی از قفل های هوشمند وجود دارد که هر کدام مزایا و معایب خاص خود را دارند. برخی از محبوب ترین انواع قفل های هوشمند عبارتند از:
 - قفل های کدی: این قفل ها با استفاده از یک کد عددی برای باز و بسته کردن درب ها استفاده می کنند. کدها معمولاً 4 تا 8 رقمی هستند و می توان آنها را به دلخواه تغییر داد. قفل های کدی نسبتاً ارزان هستند و نصب آنها آسان است. با این حال، آنها ممکن است ایمن ترین گزینه نباشند، زیرا کدها می توانند توسط افراد دیگر هک شوند.
- قفل های کارتی: این قفل ها با استفاده از یک کارت RFID برای باز و بسته کردن درب ها استفاده می کنند. کارت ها معمولاً حاوی یک تراشه کوچک هستند که با قفل ارتباط برقرار می کند. قفل های کارتی ایمن تر از قفل های کدی هستند، زیرا کارت ها دشوارتر از کدها هک می شوند. با این حال، آنها ممکن است کمی گران تر از قفل های کدی باشند.
- قفل های اثر انگشت: این قفل ها با استفاده از اثر انگشت کاربر برای باز و بسته کردن درب ها استفاده می کنند. اثر انگشت ها منحصر به فرد هستند و بنابراین نسبتاً ایمن هستند. قفل های اثر انگشت راحت هستند، زیرا نیازی به حمل کارت یا وارد کردن کد ندارید. با این حال، آنها ممکن است کمی گران تر از قفل های کدی یا کارتی باشند.
- قفل های تشخیص چهره: این قفل ها با استفاده از تشخیص چهره کاربر برای باز و بسته کردن درب ها استفاده می کنند. تشخیص چهره می تواند ایمن تر از اثر انگشت باشد زیرا نمی توان آن را به راحتی با یک عکس جعلی کرد. قفل های تشخیص چهره راحت هستند، زیرا نیازی به حمل کارت یا وارد کردن کد ندارید. با این حال، آنها ممکن است گران ترین نوع قفل هوشمند باشند.
- ویژگی های امنیتی: برخی از قفل های هوشمند از ویژگی های امنیتی اضافی مانند تأیید دو مرحله ای یا هشدارهای امنیتی برخوردار هستند که می توانند امنیت را افزایش دهند.
- سازگاری با دستگاه های دیگر: برخی از قفل های هوشمند فقط با دستگاه های خاصی سازگار هستند. قبل از خرید، مطمئن شوید که قفل شما با دستگاه های شما سازگار است.
- هزینه: قفل های هوشمند می توانند از چند صد هزار تومان تا چند میلیون تومان قیمت داشته باشند. قبل از خرید، بودجه خود را در نظر بگیرید.

نکات مهم در استفاده از قفل های هوشمند

پس از خرید قفل هوشمند، مهم است که نکات زیر را برای استفاده ایمن از قفل خود دنبال کنید:

- رمزهای عبور قوی استفاده کنید. از رمزهای عبور قوی استفاده کنید که شامل حداقل 8 کاراکتر از حروف بزرگ، حروف کوچک، اعداد و نمادها باشند.
- رمزهای عبور خود را به طور منظم تغییر دهید. رمزهای عبور خود را به طور منظم تغییر دهید تا از هک شدن آنها جلوگیری کنید.
- کارت ها و اثر انگشت ها را ایمن نگه دارید. کارت ها و اثر انگشت های خود را ایمن نگه دارید تا دیگران نتوانند از آنها برای باز کردن قفل شما استفاده کنند.
- قفل خود را به روز نگه دارید. سازنده قفل شما معمولاً به روزرسانی های نرم افزاری را برای قفل خود منتشر می کند. این به روزرسانی ها می توانند شامل رفع اشکالات و بهبود امنیت باشند. با پیروی از این نکات، می توانید از قفل هوشمند خود و اطلاعات شخصی خود محافظت کنید.

برترین قفل هوشمند

Samsung SDS SHP-DP728

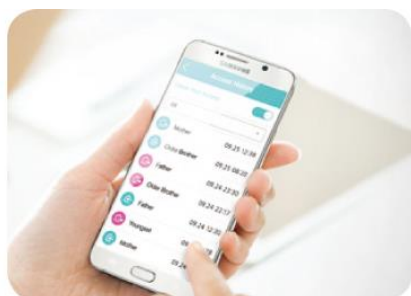


- قابلیت نصب سیستم بلوتوث برای ۸ کاربر و ۳ قفل
- استفاده از رمز عبوری ۴ تا ۱۲ رقمی به طور رندوم و صفحه لمسی مدرن و زیبا
- دسترسی به قفل توسط رمز عبوری کارت یا تگ RF برای ۳۱ کاربر
- قابلیت ذخیره ۱۰۰ اثر انگشت (Finger Print)
- قابلیت استفاده همزمان رمز عبوری و اثر انگشت بصورت ترکیبی
- از قسمت داخلی با کشیدن دستگیره هم درب و هم قفل باز می شوند (pull).
- مجهز به سیستم هوشمند اینفرارد جهت فعال شدن قفل از فاصله ۷۰ سانتیمتری
- مجهز به درب اتوماتیک محافظ سنسور اثر انگشت
- از قسمت بیرونی با فشار دادن دستگیره هم درب و هم قفل باز می شوند (push) .
- منبع تغذیه قفل به وسیله باتری های قلمی AA و مجهز به سیستم تغذیه اضطراری
- مجهز به سنسور اعلام حریق و آلام دزدگیر
- مجهز به قفل مکانیکی با کلید فلزی کامپیوتری جهت استفاده در مواقع اضطراری
- قابلیت نصب سیستم ریموت کنترل از راه دور (option)
- مجهز به سیستم ضد سرقت



سلامت و بازگشت اعضای خانواده خود را از طریق پیام های سرویس در هر زمان متوجه شوید .
اطلاع از زمان دقیق ورود و خروج اعضای خانواده به منزل با استفاده از اپلیکیشن sHome

دیگر نیازی به همراه داشتن تگ و کارت نیست با موبایل هوشمند خود به قفل الکترونیکی خود نزدیک شوید و با لمس یک دکمه از طریق اپلیکیشن sHome درب منزل خود را باز کنید.



افزایش امنیت منازل از طریق ثبت ورود و خروج شما قادر خواهید بود تا ثبت بیش از ۳۰ ورود و خروج را از طریق اپلیکیشن sHome ملاحظه کنید

عملکرد آسان در باز شدن درب در هنگام ورود



با دارا بودن تکنولوژی IR (اینفرارد) بصورت اتوماتیک قادر به تشخیص هر حرکتی از فاصله ۵۰ سانتیمتری می باشد و قفل آماده ثبت اثر انگشت ،رمز و یا کارت جهت باز شدن درب خواهد بود.

در شرایط اضطراری نظیر آتشسوزی و زلزله دستگیره اهرمی به شما امکان خروج سریع و سالم از منزل را خواهد داد



با فشار ساده یک دکمه خانه بعد از قفل شدن درب، چنانچه افراد غریبه از راه های دیگر وارد منزل شما شده باشند، به محض باز کردن درب از سمت داخل آلامر دزدگیر فعال خواهد شد.



ظاهر شدن پیام باز یا بسته بودن قفل بر روی صفحه



زمانیکه سنسور IR حرکت مشکوکی را بیش از زمان ۱ دقیقه تشخیص دهد آلامر اعلام خطر فعال خواهد شد



تاییدیه جهانی تکنولوژی و کیفیت سامسونگ
مجهز به مغزی دو زبانه!



اثر انگشت

تا 100 اثر انگشت را بدون تاخیر و اشتباه ذخیره و باز میکند



(option) قابلیت نصب سیستم ریموت کنترل از راه دور
شامل دستگاه ریموت کنترل و برد الکترونیکی



معیارهای انتخاب قفل های هوشمند

قفل های هوشمند مزایای زیادی نسبت به قفل های سنتی دارند، از جمله:

- امنیت بالاتر: قفل های هوشمند از فناوری های امنیتی پیشرفته ای مانند اثر انگشت، تشخیص چهره و رمز عبور استفاده می کنند که می توانند امنیت خانه یا محل کار شما را به میزان قابل توجهی افزایش دهند.
 - راحتی بیشتر: قفل های هوشمند نیاز به استفاده از کلید را از بین می برند، بنابراین می توانید درب ها را با استفاده از تلفن همراه، اثر انگشت یا سایر روش های بیومتریک باز کنید.
 - قابلیت کنترل از راه دور: قفل های هوشمند را می توان از راه دور با استفاده از تلفن همراه یا سایر دستگاه های هوشمند کنترل کرد. این ویژگی می تواند برای باز کردن درب ها برای مهمانان یا کنترل دسترسی به خانه یا محل کار شما از راه دور مفید باشد.
- با این حال، قفل های هوشمند نیز می توانند هزینه بیشتری نسبت به قفل های سنتی داشته باشند و ممکن است نیاز به نصب تخصصی داشته باشند.
- در اینجا برخی از معیارهای مهمی که باید هنگام انتخاب قفل هوشمند در نظر بگیرید آورده شده است: نوع قفل: انواع مختلفی از قفل های هوشمند وجود دارد که هر کدام مزایا و معایب خاص خود را دارند. برخی از محبوب ترین انواع قفل های هوشمند عبارتند از:
- قفل های کدی: این قفل ها با استفاده از یک کد عددی برای باز و بسته کردن درب ها استفاده می کنند. کدها معمولاً 4 تا 8 رقمی هستند و می توان آنها را به دلخواه تغییر داد. قفل های کدی نسبتاً ارزان هستند و نصب آنها آسان است. با این حال، آنها ممکن است ایمن ترین گزینه نباشند، زیرا کدها می توانند توسط افراد دیگر هک شوند.
 - قفل های کارتی: این قفل ها با استفاده از یک کارت RFID برای باز و بسته کردن درب ها استفاده می کنند. کارت ها معمولاً حاوی یک تراشه کوچک هستند که با قفل ارتباط برقرار می کند. قفل های کارتی ایمن تر از قفل های کدی هستند، زیرا کارت ها دشوارتر از کدها هک می شوند. با این حال، آنها ممکن است کمی گران تر از قفل های کدی باشند.
 - قفل های اثر انگشت: این قفل ها با استفاده از اثر انگشت کاربر برای باز و بسته کردن درب ها استفاده می کنند. اثر انگشت ها منحصر به فرد هستند و بنابراین نسبتاً ایمن هستند. قفل های اثر انگشت راحت هستند، زیرا نیازی به حمل کارت یا وارد کردن کد ندارید. با این حال، آنها ممکن است کمی گران تر از قفل های کدی یا کارتی باشند.
 - قفل های تشخیص چهره: این قفل ها با استفاده از تشخیص چهره کاربر برای باز و بسته کردن درب ها استفاده می کنند. تشخیص چهره می تواند ایمن تر از اثر انگشت باشد زیرا نمی توان آن را

به راحتی با یک عکس جعلی کرد. قفل های تشخیص چهره راحت هستند، زیرا نیازی به حمل کارت یا وارد کردن کد ندارید. با این حال، آنها ممکن است گران ترین نوع قفل هوشمند باشند. ویژگی های امنیتی: برخی از قفل های هوشمند از ویژگی های امنیتی اضافی مانند تأیید دو مرحله ای یا هشدارهای امنیتی برخوردار هستند که می توانند امنیت را افزایش دهند. سازگاری با دستگاه های دیگر: برخی از قفل های هوشمند فقط با دستگاه های خاصی سازگار هستند. قبل از خرید، مطمئن شوید که قفل شما با دستگاه های شما سازگار است. هزینه: قفل های هوشمند می توانند از چند صد هزار تومان تا چند میلیون تومان قیمت داشته باشند. قبل از خرید، بودجه خود را در نظر بگیرید. عمر باتری: قفل های هوشمند معمولاً با باتری کار می کنند. قبل از خرید، مطمئن شوید که عمر باتری قفل برای نیازهای شما کافی است. قابلیت نصب: برخی از قفل های هوشمند نیاز به نصب تخصصی دارند. قبل از خرید، مطمئن شوید که می توانید قفل را خودتان نصب کنید یا باید از یک متخصص کمک بگیرید. گارانتی: قفل های هوشمند معمولاً با گارانتی همراه هستند. قبل از خرید، مطمئن شوید که گارانتی قفل شامل چه مواردی می شود. با در نظر گرفتن این معیارها می توانید قفل هوشمندی را انتخاب کنید که نیازها و بودجه شما را برآورده کند.

محصولات برتر در بازار

6 مدل قفل هوشمند پرفروش و امتیاز بالا در بازار

در ادامه به بررسی 6 مدل قفل هوشمند پرفروش و امتیاز بالا در بازار می پردازیم. این قفل ها از نظر نوع، ویژگی ها، قیمت و امتیازات کاربران مورد بررسی قرار گرفته اند.

1. قفل هوشمند سامسونگ مدل SHP-DP728

قفل هوشمند سامسونگ مدل SHP-DP728 یکی از پرفروش ترین قفل های هوشمند در بازار است. این قفل از نوع اثر انگشت و کارتی است و دارای ویژگی های امنیتی متعددی مانند تأیید دو مرحله ای و هشدارهای امنیتی است. همچنین، این قفل با دستگاه های اندروید و iOS سازگار است و از طریق برنامه تلفن همراه قابل کنترل است.

نقاط مثبت:

- امنیت بالا
- سازگاری با دستگاه های اندروید و iOS
- قابلیت کنترل از راه دور

نقاط منفی:

- قیمت بالا
- نیاز به نصب تخصصی

2. قفل هوشمند یوکا مدل YSL-368

قفل هوشمند یوکا مدل YSL-368 یکی دیگر از قفل های هوشمند پرفروش در بازار است. این قفل از نوع اثر انگشت و کارتی است و دارای ویژگی های امنیتی متعددی مانند تأیید دو مرحله ای و هشدارهای امنیتی است. همچنین، این قفل با دستگاه های اندروید و iOS سازگار است و از طریق برنامه تلفن همراه قابل کنترل است.

نقاط مثبت:

- امنیت بالا
- سازگاری با دستگاه های اندروید و iOS
- قابلیت کنترل از راه دور

نقاط منفی:

- قیمت نسبتاً بالا
- نیاز به نصب تخصصی

3. قفل هوشمند یال مدل 4109

قفل هوشمند یال مدل 4109 یکی از قفل های هوشمند با کیفیت و قیمت مناسب در بازار است. این قفل از نوع اثر انگشت و کارتی است و دارای ویژگی های امنیتی متعددی مانند تأیید دو مرحله ای و هشدارهای امنیتی است. همچنین، این قفل با دستگاه های اندروید و iOS سازگار است و از طریق برنامه تلفن همراه قابل کنترل است.

نقاط مثبت:

- کیفیت بالا
- قیمت مناسب
- امنیت بالا

نقاط منفی:

- سازگاری با دستگاه های محدود
- نیاز به نصب تخصصی

4. قفل هوشمند میلر مدل 700

قفل هوشمند میلر مدل 700 یکی از قفل های هوشمند با امنیت بالا و قیمت مناسب در بازار است. این قفل از نوع اثر انگشت، کارتی و رمزی است و دارای ویژگی های امنیتی متعددی مانند تأیید دو مرحله ای و هشدارهای امنیتی است. همچنین، این قفل با دستگاه های اندروید و iOS سازگار است و از طریق برنامه تلفن همراه قابل کنترل است.

نقاط مثبت:

- امنیت بالا
- قیمت مناسب
- سازگاری با دستگاه های اندروید و iOS

نقاط منفی:

- نیاز به نصب تخصصی
- قابلیت کنترل از راه دور محدود

5. قفل هوشمند Schlage Sense مدل BE469

قفل هوشمند Schlage Sense مدل BE469 یکی از قفل های هوشمند با طراحی زیبا و کیفیت بالا در بازار است. این قفل از نوع اثر انگشت، کارتی و رمزی است و دارای ویژگی های امنیتی متعددی مانند تأیید دو مرحله ای و هشدارهای امنیتی است. همچنین، این قفل با دستگاه های اندروید و iOS سازگار است و از طریق برنامه تلفن همراه قابل کنترل است.

نقاط مثبت:

- طراحی زیبا

- کیفیت بالا

- امنیت بالا

نقاط منفی:

- قیمت نسبتاً بالا

- نیاز به نصب تخصصی

6. قفل هوشمند ویرا مدل V100

قفل هوشمند ویرا مدل V100 یکی از قفل های هوشمند با قیمت مناسب و قابلیت های کاربردی در بازار است. این قفل از نوع اثر انگشت، کارتی و رمزی است و دارای ویژگی های امنیتی متعددی مانند تأیید دو مرحله ای و هشدارهای امنیتی است. همچنین، این قفل با دستگاه های اندروید و iOS سازگار است و از طریق برنامه تلفن همراه قابل کنترل است.

نقاط مثبت:

- قیمت مناسب

- قابلیت های کاربردی

- سازگاری با دستگاه های اندروید و iOS

نقاط منفی:

- امنیت نسبتاً پایین

- نیاز به نصب تخصصی

قفل های هوشمند دسترسی به اینترنت

اتصال به اینترنت

قفل های هوشمند با این قابلیت امکان کنترل و مدیریت از راه دور را فراهم می کنند

تلفن هوشمند

با استفاده از تلفن هوشمند می توانید به صورت راه دور قفل خود را باز و ببندید

اطلاع رسانی هوشمند

قفل های هوشمند می توانند به شما اعلان دهند که کدام افراد به خانه یا دفتر شما وارد شده اند یا خارج شده اند

قفل های هوشمند و امنیت

تشخیص اثر انگشت

قفل های هوشمند با تشخیص اثر انگشت می توانند از برخورداری از امنیت بیشتر نسبت به رمز عبور برخوردار باشند.

انتقال رمز عبور

امکان انتقال رمز عبور درونی قفل های هوشمند از طریق پشتیبانی از دستگاه های هوشمند توسط کاربر را فراهم می کنند.

حضور فیزیکی

در صورتی که قفل هوشمند دسترسی بدون تماس فیزیکی را فراهم نکند امنیت بالاتری را برای شما فراهم خواهد کرد.

PEAS معنای اختصار

Sensors، (عملگرها) Actuators، (محیط) Environment، (اندازه گیری عملکرد) Performance measure مخفف PEAS برای تعریف سیستم های هوشمند و تعیین عملکرد آنها استفاده می شوند. در قفل های PEAS (سنسورها) است. عناصر هوشمند نیز این عناصر مورد استفاده قرار می گیرند.

در قفل های هوشمند PEAS مفهوم عناصر

PEAS مخفف Protection، Ease of Use، Access و Security است. اینها چهار اصل اصلی هستند که باید هنگام خرید قفل هوشمند در نظر گرفته شوند.

- Protection: قفل هوشمند شما باید از خانه یا محل کار شما در برابر ورود غیرمجاز محافظت کند. قفل هایی که از فناوری های امنیتی پیشرفته مانند اثر انگشت، تشخیص چهره یا رمزنگاری استفاده می کنند، امن تر از قفل هایی هستند که از روش های امنیتی سنتی استفاده می کنند.
 - Ease of Use: قفل هوشمند شما باید استفاده آسانی داشته باشد. قفل هایی که از برنامه های تلفن همراه یا سایر دستگاه های هوشمند پشتیبانی می کنند، استفاده آسان تری دارند.
 - Access: قفل هوشمند شما باید به راحتی قابل دسترسی باشد. قفل هایی که از ویژگی های دسترسی از راه دور مانند کلیدهای دیجیتال پشتیبانی می کنند، دسترسی آسان تری دارند.
 - Security: قفل هوشمند شما باید از اطلاعات شما محافظت کند. قفل هایی که از احراز هویت دو مرحله ای یا سایر ویژگی های امنیتی پشتیبانی می کنند، امنیت بیشتری دارند.
- هنگام خرید قفل هوشمند، مهم است که این چهار اصل را در نظر بگیرید تا مطمئن شوید که قفل مناسبی برای نیازهای شما انتخاب می کنید.

در قفل های هوشمند PEAS مثال های عملی از موارد استفاده از عناصر

Protection

- استفاده از فناوری های امنیتی پیشرفته

قفل های هوشمند از فناوری های امنیتی پیشرفته مانند اثر انگشت، تشخیص چهره یا رمزنگاری استفاده می کنند تا از خانه یا محل کار شما در برابر ورود غیرمجاز محافظت کنند. به عنوان مثال، قفل های اثر انگشت از الگوهای منحصر به فرد اثر انگشت شما برای شناسایی شما استفاده می کنند. قفل های تشخیص چهره از ویژگی های بیومتریک صورت شما برای شناسایی شما استفاده می کنند. و قفل های رمزنگاری از الگوریتم های رمزنگاری برای محافظت از داده های شما استفاده می کنند.

- استفاده از ویژگی های امنیتی اضافی

قفل های هوشمند همچنین می توانند از ویژگی های امنیتی اضافی مانند تأیید دو مرحله ای یا هشدارهای امنیتی استفاده کنند. تأیید دو مرحله ای یک لایه امنیتی اضافی اضافه می کند که نیاز به وارد کردن کد یا تأیید از طریق دستگاه دیگری دارد. هشدارهای امنیتی می توانند شما را در صورت وقوع فعالیت مشکوک مانند تلاش برای باز کردن قفل با استفاده از یک کد نادرست مطلع کنند.

Ease of Use

- استفاده از برنامه های تلفن همراه یا سایر دستگاه های هوشمند

قفل های هوشمند می توانند با برنامه های تلفن همراه یا سایر دستگاه های هوشمند کار کنند. این امر استفاده از قفل را آسان تر می کند زیرا می توانید قفل را از راه دور کنترل کنید یا از طریق برنامه قفل را باز کنید.

- استفاده از ویژگی های دسترسی ساده

قفل های هوشمند می توانند از ویژگی های دسترسی ساده مانند کلیدهای دیجیتالی یا کدهای ورودی استفاده کنند. این ویژگی ها می توانند دسترسی به قفل را آسان تر کنند.

Access

- استفاده از ویژگی های دسترسی از راه دور

قفل های هوشمند می توانند از ویژگی های دسترسی از راه دور مانند کلیدهای دیجیتالی یا برنامه های تلفن همراه استفاده کنند. این ویژگی ها می توانند دسترسی به قفل را از هر کجا که هستید آسان تر کنند.

- استفاده از ویژگی های دسترسی موقت

قفل های هوشمند می توانند از ویژگی های دسترسی موقت مانند کلیدهای دیجیتالی یا کدهای ورودی استفاده کنند. این ویژگی ها می توانند به شما امکان دهند به طور موقت به دیگران دسترسی به قفل خود بدهید.

Security

- استفاده از احراز هویت دو مرحله ای
- احراز هویت دو مرحله ای یک لایه امنیتی اضافی اضافه می کند که نیاز به وارد کردن کد یا تأیید از طریق دستگاه دیگری دارد. این امر می تواند امنیت قفل شما را افزایش دهد زیرا حتی اگر رمز عبور خود را به اشتباه وارد کنید، هنوز هم نمی توانید قفل را باز کنید.
- استفاده از رمزنگاری
- رمزنگاری از الگوریتم های رمزنگاری برای محافظت از داده های شما استفاده می کند. این امر می تواند از اطلاعات شخصی شما در برابر دسترسی غیرمجاز محافظت کند.
- در اینجا چند مثال خاص از نحوه استفاده از عناصر PEAS در قفل های هوشمند آورده شده است:
- یک قفل هوشمند ممکن است از اثر انگشت و رمزنگاری برای محافظت از خانه شما در برابر ورود غیرمجاز استفاده کند.
- یک قفل هوشمند دیگر ممکن است از برنامه تلفن همراه برای کنترل قفل از راه دور استفاده کند.
- یک قفل هوشمند سوم ممکن است از کلیدهای دیجیتالی برای دسترسی به قفل توسط مهمانان استفاده کند.
- با در نظر گرفتن این چهار اصل هنگام خرید قفل هوشمند، می توانید مطمئن شوید که قفل مناسبی برای نیازهای خود انتخاب می کنید.

جست و جوی نا آگاهانه در قفل های هوشمند

جستجو نا آگاهانه در قفل های هوشمند

جستجوی نا آگاهانه در قفل های هوشمند به معنای تلاش برای باز کردن قفل بدون استفاده از روشی که توسط سازنده قفل مجاز است. این می تواند شامل تلاش برای باز کردن قفل با استفاده از یک کلید جعلی، تلاش برای باز کردن قفل با استفاده از ابزاری مانند یک پیچ گوشتی یا تلاش برای باز کردن قفل با استفاده از یک روش نرم افزاری مانند حملات Brute Force باشد.

جستجوی نا آگاهانه در قفل های هوشمند می تواند منجر به آسیب به قفل یا حتی شکستن آن شود. همچنین می تواند منجر به نقض امنیت شود و به سارقان اجازه دهد به خانه یا محل کار شما دسترسی پیدا کنند.

برای جلوگیری از جستجوی نا آگاهانه در قفل های هوشمند، مهم است که اقدامات احتیاطی زیر را انجام دهید:

- از قفل های هوشمند با ویژگی های امنیتی پیشرفته استفاده کنید. این ویژگی ها می توانند امنیت قفل شما را در برابر حملات جستجوی نا آگاهانه افزایش دهند.
- رمزهای عبور قوی ایجاد کنید. از رمزهای عبوری استفاده کنید که حداقل 8 کاراکتر داشته باشند و شامل ترکیبی از حروف بزرگ، حروف کوچک، اعداد و نمادها باشند.
- رمزهای عبور خود را به طور منظم تغییر دهید. این به جلوگیری از دسترسی افراد غیرمجاز کمک می کند.
- از ویژگی های امنیتی اضافی مانند احراز هویت دو مرحله ای استفاده کنید. احراز هویت دو مرحله ای یک لایه امنیتی اضافی اضافه می کند که نیاز به وارد کردن کد یا تأیید از طریق دستگاه دیگری دارد.
- قفل خود را به روز نگه دارید. سازنده قفل شما معمولاً به روزرسانی های نرم افزاری را برای قفل خود منتشر می کند. این به روزرسانی ها می توانند شامل رفع اشکالات و بهبود امنیت باشند. با انجام این اقدامات احتیاطی، می توانید امنیت قفل هوشمند خود را در برابر جستجوی نا آگاهانه افزایش دهید.

راه های جلوگیری از جستجوی نا آگاهانه در قفل های هوشمند

در اینجا چند راه برای جلوگیری از جستجوی نا آگاهانه در قفل های هوشمند آورده شده است:

- از قفل های هوشمند با ویژگی های امنیتی پیشرفته استفاده کنید. این ویژگی ها می توانند امنیت قفل شما را در برابر حملات جستجوی نا آگاهانه افزایش دهند. برخی از ویژگی های امنیتی پیشرفته که می توانند به جلوگیری از جستجوی نا آگاهانه کمک کنند عبارتند از:
 - رمزنگاری: رمزنگاری از داده های شما در برابر دسترسی غیرمجاز محافظت می کند.

- احراز هویت دو مرحله ای: احراز هویت دو مرحله ای یک لایه امنیتی اضافی اضافه می کند که نیاز به وارد کردن کد یا تأیید از طریق دستگاه دیگری دارد.
- تشخیص نفوذ: تشخیص نفوذ می تواند شما را در صورت وقوع فعالیت مشکوک مانند تلاش برای باز کردن قفل با استفاده از یک کد نادرست مطلع کند.
- رمزهای عبور قوی ایجاد کنید. از رمزهای عبوری استفاده کنید که حداقل 8 کاراکتر داشته باشند و شامل ترکیبی از حروف بزرگ، حروف کوچک، اعداد و نمادها باشند. رمزهای عبور قوی تر دشوارتر برای حدس زدن هستند.
- رمزهای عبور خود را به طور منظم تغییر دهید. این به جلوگیری از دسترسی افراد غیرمجاز کمک می کند.
- از ویژگی های امنیتی اضافی مانند کلیدهای دیجیتالی یا برنامه تلفن همراه استفاده کنید. این ویژگی ها می توانند دسترسی به قفل شما را محدود کنند و به جلوگیری از جستجوی نا آگاهانه کمک کنند.
- قفل خود را به روز نگه دارید. سازنده قفل شما معمولاً به روزرسانی های نرم افزاری را برای قفل خود منتشر می کند. این به روزرسانی ها می توانند شامل رفع اشکالات و بهبود امنیت باشند. با انجام این اقدامات احتیاطی، می توانید امنیت قفل هوشمند خود را در برابر جستجوی نا آگاهانه افزایش دهید.

مسائل ارضای محدودیت در قفل های هوشمند

مسائل ارضای محدودیت در قفل های هوشمند

قفل های هوشمند دستگاه های پیچیده ای هستند که باید مجموعه ای از محدودیت ها را برآورده کنند. برخی از این محدودیت ها عبارتند از:

- امنیت: قفل های هوشمند باید در برابر حملات مختلف، از جمله حملات جستجوی نا آگاهانه، ایمن باشند.
- راحتی استفاده: قفل های هوشمند باید برای کاربران راحت و آسان برای استفاده باشند.
- قابلیت اطمینان: قفل های هوشمند باید قابل اعتماد باشند و به طور مداوم کار کنند.
- صرفه جویی در انرژی: قفل های هوشمند باید انرژی کمی مصرف کنند تا عمر باتری طولانی داشته باشند.

ارضای این محدودیت ها می تواند چالش برانگیز باشد. به عنوان مثال، برای افزایش امنیت قفل، می توان از ویژگی هایی مانند رمزنگاری و احراز هویت دو مرحله ای استفاده کرد. این ویژگی ها می توانند امنیت قفل را افزایش دهند، اما همچنین می توانند استفاده از قفل را برای کاربران دشوارتر کنند. در اینجا برخی از مسائل ارضای محدودیت در قفل های هوشمند آورده شده است:

- موازنه بین امنیت و راحتی استفاده: قفل های هوشمند باید ایمن باشند، اما همچنین باید برای کاربران راحت و آسان برای استفاده باشند. یافتن تعادل بین این دو چالش برانگیز است.
 - موازنه بین امنیت و صرفه جویی در انرژی: قفل های هوشمند باید ایمن باشند، اما همچنین باید انرژی کمی مصرف کنند تا عمر باتری طولانی داشته باشند. یافتن تعادل بین این دو نیز چالش برانگیز است.
 - موازنه بین قابلیت اطمینان و هزینه: قفل های هوشمند باید قابل اعتماد باشند، اما همچنین باید مقرون به صرفه باشند. یافتن تعادل بین این دو نیز چالش برانگیز است.
- سازندگان قفل های هوشمند با تلاش برای یافتن راه حل هایی برای این مسائل، به طور مداوم در حال بهبود قفل های هوشمند خود هستند.

عامل مبتنی بر حل مساله انواع مساله

. فرموله سازی مساله

. انواع جستجوهای ناآگاهان

عامل مبتنی بر حل مساله

عامل مبتنی بر حل مساله یک نوع عامل هوش مصنوعی است که برای حل مشکلات پیچیده طراحی شده است. این عوامل با فرموله کردن مشکل به عنوان یک مسئله جستجو و سپس استفاده از یک الگوریتم جستجو برای یافتن راه حل کار می کنند.

انواع مساله

مسائلی که می توانند توسط عوامل مبتنی بر حل مساله حل شوند، می توانند بسیار متنوع باشند. برخی از انواع رایج مسائل عبارتند از:

- مسائل جستجوی حالت: در این نوع مسائل، هدف یافتن یک مسیر از یک حالت اولیه به یک حالت هدف است. به عنوان مثال، یک عامل مبتنی بر حل مساله می تواند برای یافتن مسیری برای یک روبات از یک نقطه شروع به یک نقطه پایانی استفاده شود.
- مسائل برنامه ریزی: در این نوع مسائل، هدف یافتن یک برنامه برای انجام یک مجموعه از وظایف است. به عنوان مثال، یک عامل مبتنی بر حل مساله می تواند برای یافتن یک برنامه برای جمع آوری یک سبد خرید از یک فروشگاه استفاده شود.
- مسائل تصمیم گیری: در این نوع مسائل، هدف یافتن بهترین تصمیم از بین یک مجموعه از گزینه ها است. به عنوان مثال، یک عامل مبتنی بر حل مساله می تواند برای یافتن بهترین مسیر برای یک خودرو در یک ترافیک سنگین استفاده شود.

فرموله سازی مساله

- گام اول در حل یک مشکل با استفاده از یک عامل مبتنی بر حل مساله، فرموله کردن مشکل به عنوان یک مسئله جستجو است. این شامل تعریف فضای حالت، تابع انتقال، تابع پاداش و هدف است.
- فضای حالت: فضای حالت مجموعه ای از تمام حالت های ممکن است که سیستم می تواند در آن قرار داشته باشد. به عنوان مثال، در مسئله جستجوی حالت، فضای حالت مجموعه ای از تمام موقعیت های ممکن روبات است.

- تابع انتقال: تابع انتقال مشخص می کند که در صورت انجام یک عمل خاص، سیستم از یک حالت به چه حالت دیگری منتقل می شود. به عنوان مثال، در مسئله جستجوی حالت، تابع انتقال مشخص می کند که در صورت حرکت روبات به یک جهت خاص، روبات به چه موقعیت جدیدی منتقل می شود.
- تابع پاداش: تابع پاداش مقداری را به هر حالت اختصاص می دهد. این تابع برای ارزیابی کیفیت یک حالت استفاده می شود. به عنوان مثال، در مسئله جستجوی حالت، تابع پاداش ممکن است مقدار فاصله روبات از حالت هدف را تعیین کند.
- هدف: هدف مشخص می کند که عامل باید چه حالتی را پیدا کند. در مسئله جستجوی حالت، هدف یافتن حالت هدف است.

انواع جستجوهای ناآگاهانه

جستجوی ناآگاهانه یک نوع الگوریتم جستجو است که از هیچ دانشی در مورد ساختار فضای جستجو استفاده نمی کند. این الگوریتم ها معمولاً ساده تر از الگوریتم های آگاهانه هستند، اما می توانند برای یافتن راه حل برای مسائل پیچیده زمان زیادی صرف کنند.

برخی از انواع رایج جستجوهای ناآگاهانه عبارتند از:

- جستجوی عمق اول: در این الگوریتم، عامل از یک حالت شروع می کند و به طور عمودی به حالت های بعدی حرکت می کند. عامل تا زمانی که به یک حالت هدف برسد یا به یک حالت بدون خروجی برسد، به حرکت ادامه می دهد.
 - جستجوی عرض اول: در این الگوریتم، عامل از یک حالت شروع می کند و به طور عرضی به حالت های بعدی حرکت می کند. عامل تا زمانی که به یک حالت هدف برسد یا به یک حالت بدون خروجی برسد، به حرکت ادامه می دهد.
 - جستجوی درجه اول: در این الگوریتم، عامل از یک حالت شروع می کند و به طور تصادفی به حالت های بعدی حرکت می کند. عامل تا زمانی که به یک حالت هدف برسد یا به یک حالت بدون خروجی برسد، به حرکت ادامه می دهد.
- جستجوی ناآگاهانه می تواند برای حل طیف وسیعی از مسائل استفاده شود. با این حال، مهم است که توجه داشته باشید که این الگوریتم ها ممکن است برای مسائل پیچیده زمان زیادی صرف کنند.

•تعریف تعریف مسایل ارضای محدودیت

•انواع مسایل ارضای محدودیت

•جستجوی عقبگرد

•بهبود جستجو

تعریف مسائل ارضای محدودیت

مسائل ارضای محدودیت (Constraint Satisfaction Problems) یا CSPها، مسائلی هستند که در آن باید مجموعه ای از متغیرها را با مقادیری تخصیص دهیم به گونه ای که مجموعه ای از محدودیت ها را برآورده کنند. به عنوان مثال، مسئله رنگ آمیزی نقشه یک CSP است که در آن باید هر کشور را با یک رنگ متفاوت رنگ آمیزی کنیم به گونه ای که هیچ دو کشور همسایه رنگ یکسانی نداشته باشند. انواع مسائل ارضای محدودیت

مسائل ارضای محدودیت را می توان به دو دسته کلی تقسیم کرد:

- مسائل CSP با متغیرهای گسسته: در این مسائل، دامنه هر متغیر یک مجموعه گسسته از مقادیر است. به عنوان مثال، مسئله رنگ آمیزی نقشه یک CSP با متغیرهای گسسته است زیرا دامنه هر کشور یک مجموعه از رنگ های مجاز است.
- مسائل CSP با متغیرهای پیوسته: در این مسائل، دامنه هر متغیر یک مجموعه پیوسته از مقادیر است. به عنوان مثال، مسئله یافتن مسیری برای یک روبات در یک فضای سه بعدی یک CSP با متغیرهای پیوسته است زیرا موقعیت هر نقطه در فضای سه بعدی یک مقدار پیوسته است.

جستجوی عقبگرد

جستجوی عقبگرد (Backtracking) یک الگوریتم کلی برای حل مسائل ارضای محدودیت است. این الگوریتم از یک فرآیند بازگشتی برای بررسی تمام راه حل های ممکن استفاده می کند. در جستجوی عقبگرد، الگوریتم از یک حالت اولیه شروع می کند و به طور تدریجی متغیرها را تخصیص می دهد. در هر مرحله، الگوریتم بررسی می کند که آیا تخصیص فعلی محدودیت ها را برآورده می کند یا خیر. اگر محدودیت ها برآورده شوند، الگوریتم به مرحله بعدی می رود. اگر محدودیت ها برآورده نشوند، الگوریتم به مرحله قبل باز می گردد و یک تخصیص متفاوت را امتحان می کند. جستجوی عقبگرد یک الگوریتم ساده و انعطاف پذیر است که می تواند برای حل طیف وسیعی از مسائل ارضای محدودیت استفاده شود. با این حال، این الگوریتم می تواند برای مسائل پیچیده زمان زیادی صرف کند.

بهبود جستجو

برای بهبود کارایی جستجوی عقبگرد، می توان از تکنیک های مختلفی استفاده کرد. برخی از این تکنیک ها عبارتند از:

- رتبه بندی متغیرها: رتبه بندی متغیرها به الگوریتم اجازه می دهد تا متغیرهایی را که احتمال بیشتری دارد که منجر به راه حل شوند، زودتر تخصیص دهد.
 - حذف حالات نامعتبر: حذف حالات نامعتبر به الگوریتم اجازه می دهد تا از بررسی راه حل هایی که از ابتدا غیرممکن هستند، جلوگیری کند.
 - انتشار محدودیت ها: انتشار محدودیت ها به الگوریتم اجازه می دهد تا محدودیت ها را به متغیرهای دیگر اعمال کند. این می تواند به الگوریتم کمک کند تا راه حل هایی را سریعتر پیدا کند.
- با استفاده از این تکنیک ها، می توان کارایی جستجوی عقبگرد را برای مسائل پیچیده به میزان قابل توجهی بهبود بخشید.

سایت های رفرنس برای کمک تولید مقاله قفل های هوشمند آورده شده است:

1. IEEE Xplore
2. ScienceDirect
3. SpringerLink
4. ACM Digital Library
5. IEEE Access
6. Nature
7. Science
8. PLOS ONE
9. IEEE Sensors Journal
10. IEEE Transactions on Consumer Electronics

این سایت ها مقالات معتبری را در زمینه قفل های هوشمند منتشر می کنند. مقالات این سایت ها توسط متخصصان این حوزه بررسی و ارزیابی می شوند و از کیفیت بالایی برخوردار هستند.

در اینجا توضیح مختصری در مورد هر یک از این سایت ها آورده شده است:

- IEEE Xplore یک پایگاه داده آنلاین است که مقالات مجلات و کنفرانس های IEEE را در زمینه های مختلف علمی و مهندسی منتشر می کند.
- ScienceDirect یک پایگاه داده آنلاین است که مقالات مجلات و کنفرانس های Elsevier را در زمینه های مختلف علمی و مهندسی منتشر می کند.
- SpringerLink یک پایگاه داده آنلاین است که مقالات مجلات و کنفرانس های Springer Nature را در زمینه های مختلف علمی و مهندسی منتشر می کند.
- ACM Digital Library یک پایگاه داده آنلاین است که مقالات مجلات و کنفرانس های Association for Computing Machinery (ACM) را در زمینه های مختلف علوم کامپیوتر منتشر می کند.
- IEEE Access یک مجله آنلاین است که مقالات در زمینه های مختلف مهندسی و علوم را منتشر می کند.
- Nature یک مجله علمی است که مقالات در زمینه های مختلف علوم طبیعی و زیست شناسی را منتشر می کند.
- Science یک مجله علمی است که مقالات در زمینه های مختلف علوم فیزیکی و زیست شناسی را منتشر می کند.
- PLOS ONE یک مجله علمی است که مقالات در زمینه های مختلف علوم را منتشر می کند.
- IEEE Sensors Journal یک مجله علمی است که مقالات در زمینه حسگرها و سیستم های حسگر را منتشر می کند.
- IEEE Transactions on Consumer Electronics یک مجله علمی است که مقالات در زمینه الکترونیک مصرفی را منتشر می کند.