شناخت و پیاده‌سازی سامانه سلامت مبتنی بر کارت هوشمند

ارائه دهنده: آرش حاجی صفی
استاد راهنما: دکتر رضا صفابخش

مرداد ۱۳۹۹

هدف ارائه

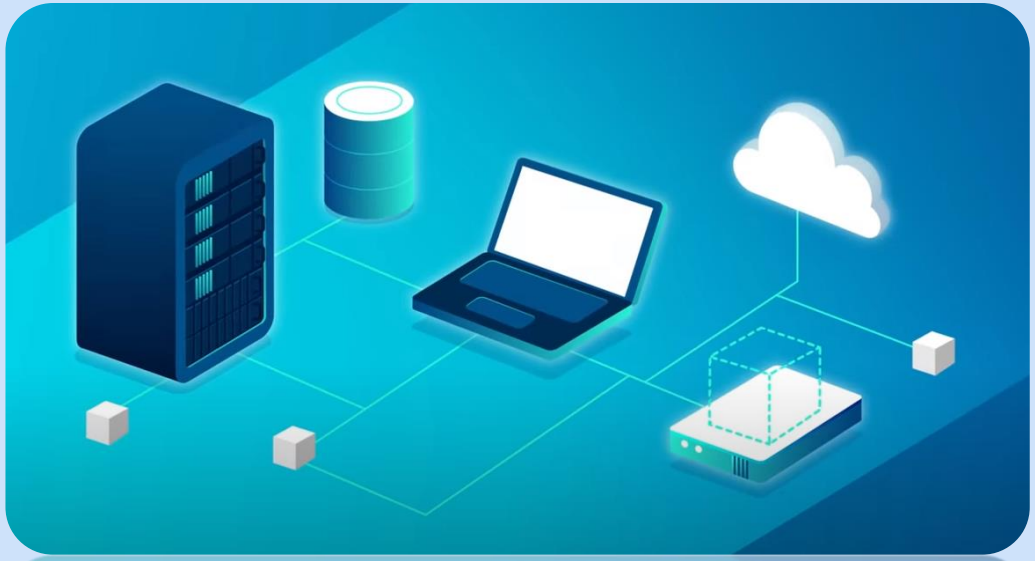
- شناخت کارت‌های هوشمند
- شناخت سلامت الکترونیک
- ارائه یک معماری برای سیستم مدیریت اطلاعات پزشکی با استفاده از کارت هوشمند، بررسی راهکارها و چالش‌ها

فهرست مطالب

مقدمه

- پراکنده بودن اطلاعات پزشکی
- چالش شرکت‌های بیمه خدمات درمانی در کشورها
- ضرورت ایجاد یک سامانه متمرکز از اطلاعات پزشکی افراد

← استفاده از کارت هوشمند



تاریخچه کارت هوشمند

۱۹۹۹

صدور اولین کارت ملی هوشمند در کشور فنلاند

۱۹۹۵

عرضه اولین نسل از سیم کارت ها

۱۹۷۶

شروع اولین اقدامات جهت توسعه کارت هوشمند برای بانک‌ها

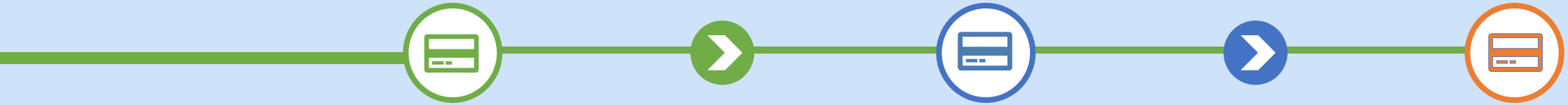
۲۰۰۱

صدور مجوز از طرف وزارت دفاع آمریکا برای به کارگیری کارت هوشمند در احراز هویت پرسنل نظامی (CAC)

۲۰۰۳

عرضه سیم کارت های میکرو

تاریخچه کارت هوشمند (ادامه)



۲۰۰۵

استفاده از اولین پاسپورت الکترونیکی منطبق با سازمان بین‌المللی هوانوردی غیر نظامی (ایکائو) در نروژ

۲۰۱۲

معرفی نانو سیم کارت ها

۲۰۱۶

عرضه اولین ساعت هوشمند با سیم کارت ادغام شده (eSIM)

کارت هوشمند

- تعریف کارت هوشمند:

+

کارت هوشمند

- تعریف کارت هوشمند:

+

SMART

کارت هوشمند (ادامه)

- ویژگی‌های کارت «هوشمند»:
  - شناسه منحصر به فرد
  - شرکت به صورت خودکار در تراکنش الکترونیکی
  - بالا بردن امنیت ← دلیل اصلی استفاده از آن
  - عدم جعل شدن به سادگی
  - نگهداری داده به صورت امن و مطمئن
  - دارای قابلیت به کارگیری الگوریتم‌ها و توابع امنیتی متفاوت
- تفاوت کارت هوشمند با کارت غیر هوشمند

تعریف سازمان بهداشت جهانی از سلامت الکترونیک

استفاده از فناوری اطلاعات و ارتباطات در حوزه سلامت جهت نگهداری، انتقال و استفاده از داده های دیجیتالی این حوزه در کاربردهای درمانی، آموزشی و اداری از طریق شبکه محلی یا راه دور

سلامت الکترونیک

- پرونده سلامت الکترونیک
  - تعریف
  - علت نیاز
    - ✓دسترسی سریع و جلوگیری از تکرار اقدامات تشخیصی
    - ✓قابلیت به اشتراک گذاری
    - ✓کاهش هزینه ها
    - ✓دانش افزایی پزشکی
    - ✓کاهش خطاهای پزشکی

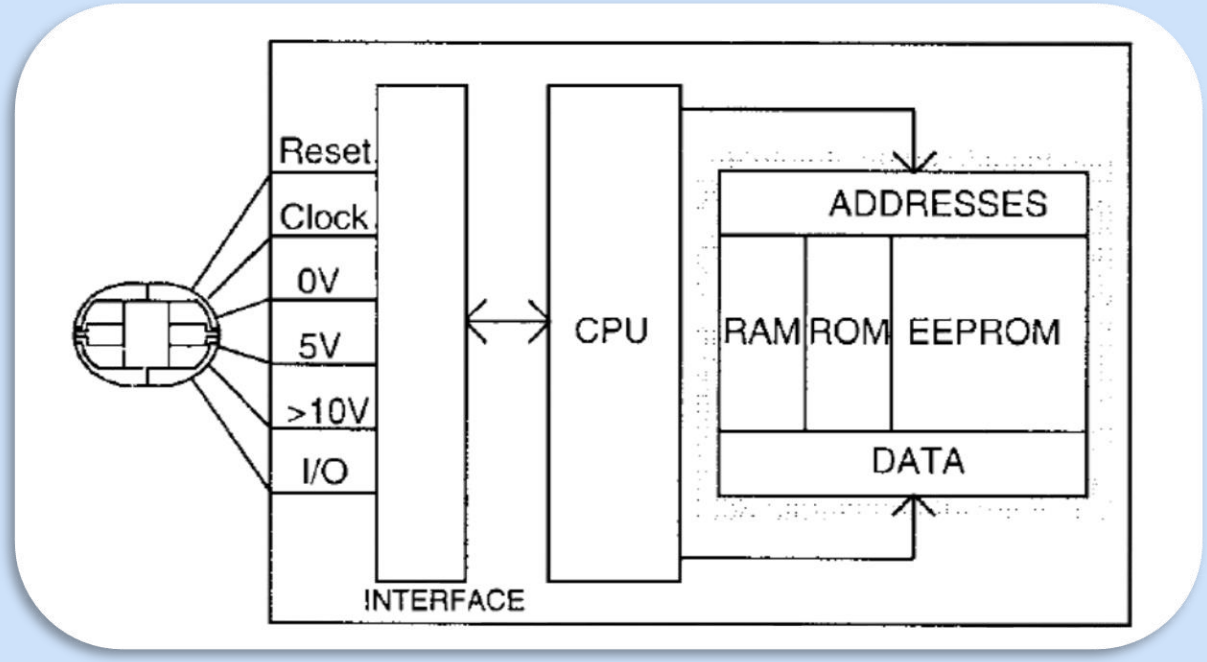
پیاده‌سازی سامانه

- کارت هوشمند سلامت:

الگوریتم‌های رمزنگاری

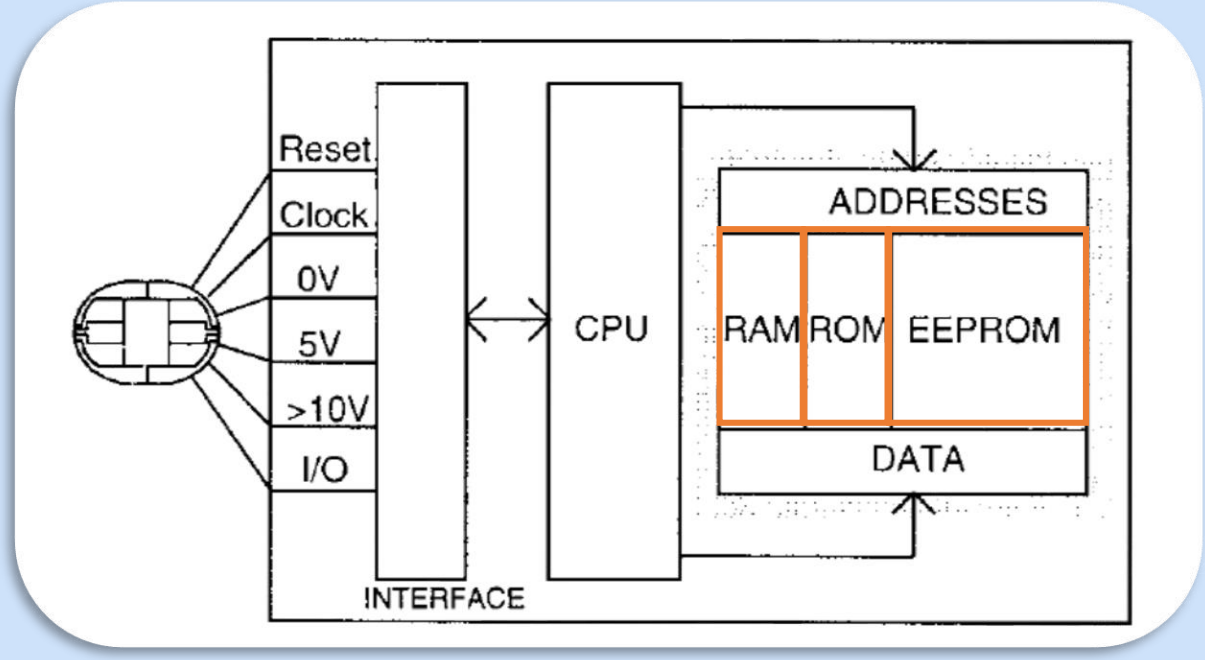
معماری کارت هوشمند سلامت

- کارت هوشمند مورد استفاده: BULL CP8
  - کارت هوشمند دارای ریزپردازنده
  - ۳ کیلوبایت حافظه برای ذخیره اطلاعات



معماری کارت هوشمند سلامت (ادامه)

- بخش‌بندی حافظه:
  - حافظه کاری
  - حافظه برنامه
    - سیستم عامل ← هوشمندی
  - حافظه کاربر
    - فضای مخفی
      - ✓کلیدهای امنیتی
    - فضای دسترسی
    - فضای عمومی
    - فضای کاری



چالش‌ها

- محدودیت حافظه ← تنها ۳ کیلوبایت فضای در دسترس برای نگهداری اطلاعات بیمار

- چالش‌های امنیتی
  - تضمین اصل محرمانگی اطلاعات
  - تضمین اصل تمامیت و صحت اطلاعات

راهکارها برای حل چالش محدودیت حافظه

- بخش‌بندی بهینه حافظه کاربر برای نگهداری سوابق بیمار
  - نگهداری هر سابقه بیماری در ۱ بیت

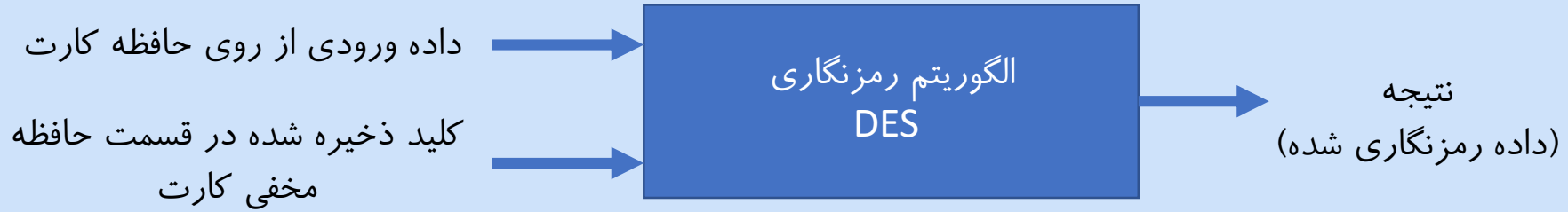
← تخصیص ۳۲ بایت از حافظه به سوابق بیماری برای نگهداری وضعیت سوابق ۲۵۶ نوع بیماری

- تخصیص یک شناسه یکتا به هر پزشک
- نگهداری اطلاعات تا حداکثر ۵۰ ویزیت

← بارگذاری اطلاعات ویزیت در هربار برقراری ارتباط کارت با سامانه سلامت الکترونیک بیمارستان

راهکارها برای تضمین اصول ایمنی

- علت اصلی استفاده از کارت‌های هوشمند
  ← قابلیت پیاده سازی الگوریتم‌های رمزنگاری
- الگوریتم رمزنگاری DES
- کلیدهای مخفی و مدیریت آنها
  - محل نگهداری کلیدها
  - نحوه تولید و بازیابی کلیدها
  - پارامترهای مورد استفاده در الگوریتم DES



راهکار تضمین محرمانگی اطلاعات

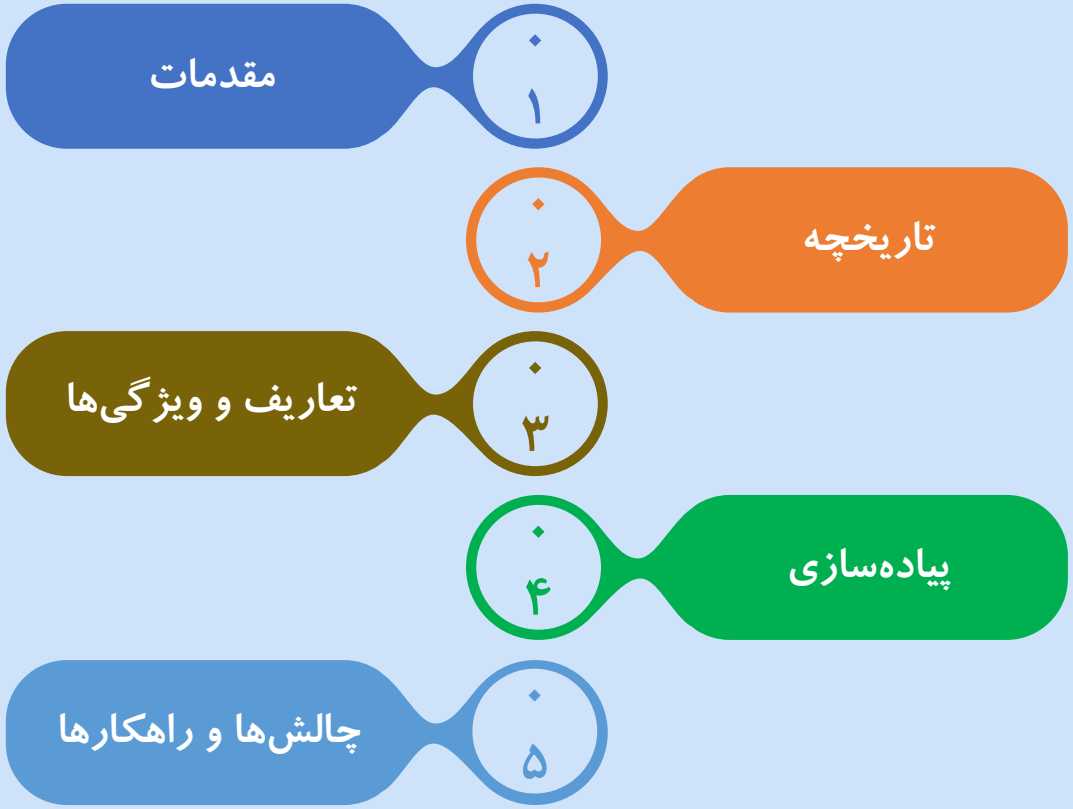
لزوم ثبت کلید مناسب برای دسترسی به قسمت‌های مختلف حافظه

- خواندن اطلاعات از کارت
  - کلید PIN
- حذف اطلاعات از کارت
  - کلید PIK
- نوشتن اطلاعات روی کارت
  - کلید CIK
  - دسترسی پزشک به ناحیه کاری ۲ از طریق کارت مخصوص

راهکار تضمین صحت اطلاعات

- حساس و حیاتی بودن اطلاعات پزشکی افراد
  - ← لزوم تضمین ۱۰۰ درصدی صحت و اعتبار اطلاعات
- تولید مقادیر CCV یا «گواه»
  - ← تضمین قطعی اصل درستی و تمامیت اطلاعات
- مکانیزم به کارگیری مقادیر CCV برای تشخیص صحت اطلاعات
- نگرانی‌های امنیتی در مورد استفاده از CCV

جمع‌بندی


۰۱
مقدمات
۰۲
تاریخچه
۰۳
تعاریف و ویژگی‌ها
۰۴
پیاده‌سازی
۰۵
چالش‌ها و راهکارها

مراجع

- C. Lambrinoudakis and S. Gritzalis, “Managing medical and insurance information through a smartcard-based information system,” *Journal of Medical Systems*, vol. 24, no. 4, pp. 213–234, 2000.
- K. E. Mayes and K. Markantonakis, *Smart cards, tokens, security and applications*, vol. 2. Springer, 2008.
- K. Häyrinen, K. Saranto, and P. Nykänen, “Definition, structure, content, use and impacts of electronic health records: a review of the research literature,” International journal of medical informatics, vol. 77, no. 5, pp. 291–304, 2008.
- R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in 2010 IEEE 3rd International Conference on cloud Computing, pp. 268–275, IEEE, 2010.

با سپاس از توجه شما ☺

اگر سوالی داشتید می‌توانید
مرا از طریق hajisafi@aut.ac.ir پیدا کنید