ISSN: 2410-7727

EVOLVING PARADIGMS IN ACCESS CONTROL SYSTEMS: INTEGRATING ADVANCED TECHNOLOGIES FOR ENHANCED SECURITY IN HEALTHCARE ENVIRONMENTS

النماذج المتطورة في أنظمة التحكم في الوصول
دمج التقنيات المتقدمة لتعزيز الأمن في بيئات الرعاية الصحية

Marwan F. S. H. AL-Kamali[1,2*]
Abdulaziz A.K. Ali[2,3]
Andrei E. Zapolski[4]

1Technical Ceramics and Nanomaterials Research Laboratories, junior research & Ph.D. associate Professor Department of "Industrial Electronics" at Sukhoi State Technical University, Gomel, 246029, Republic of Belarus., Scopus: 58547258100, https://orcid.org/0009-0004-3503-1373.
2Scientific Organization for Research and Innovation, Yemen .
3Department "Industrial Electronics"& Junior research assistant at Sukhoi State Technical University, Gomel, 246029, Republic of Belarus.
4 PhD. Student of the Department "Industrial Electronics at Sukhoi State Technical University, Gomel, 246029, Republic of Belarus.
†Corresponding author: Abdulaziz A.K. Ali; E-mail: iT.Abdulaziz@Proton.me ; Contact No.: +375 25 530-12-59

ISSN: 2410-7727

ISSN: 2410-7727

EVOLVING PARADIGMS IN ACCESS CONTROL SYSTEMS: INTEGRATING ADVANCED TECHNOLOGIES FOR ENHANCED SECURITY IN HEALTHCARE ENVIRONMENTS

Marwan F. S. H. AL-Kamali[1,2*]
Abdulaziz A.K. Ali[2,3]
Andrei E. Zapolski[4]

1Technical Ceramics and Nanomaterials Research Laboratories, junior research & Ph.D. associate Professor Department of "Industrial Electronics" at Sukhoi State Technical University, Gomel, 246029, Republic of Belarus., Scopus: 58547258100, https://orcid.org/0009-0004-3503-1373.
2Scientific Organization for Research and Innovation, Yemen .
3Department "Industrial Electronics"& Junior research assistant at Sukhoi State Technical University, Gomel, 246029, Republic of Belarus.
4 PhD. Student of the Department "Industrial Electronics at Sukhoi State Technical University, Gomel, 246029, Republic of Belarus.
†Corresponding author: Abdulaziz A.K. Ali; E-mail: iT.Abdulaziz@Proton.me ; Contact No.: +375 25 530-12-59

ABSTRACT

This study explores the evolution of Access Control Systems (ACS) and their adaptation to modern technologies, reflecting the ongoing advancements in security demands. Tracing the history of access control from simple mechanical locks in ancient civilizations to sophisticated smart technologies, we analyze the impact of innovations such as biometrics and the Internet of Things (IoT) on access management strategies. The research identifies key trends and challenges within modern ACS, pointing out cybersecurity vulnerabilities and the necessity for improved legal frameworks. The proposed model integrates smart locks with electronic health records, allowing healthcare providers secure access to patient data, thus enhancing patient care and operational efficiency. The findings emphasize the need for ongoing development and integration of modern ACS to address current challenges in the healthcare context, particularly in regions like Yemen.

Keywords: Access Control Systems (ACS), Biometric Authentication, Internet of Things (IoT), Cybersecurity, Patient Data, Management, Smart Lock Technologies, Electronic Health Records (EHR).

ISSN: 2410-7727

النماذج المتطورة في أنظمة التحكم في الوصول
دمج التقنيات المتقدمة لتعزيز الأمن في بيئات الرعاية الصحية

د. مروان فرحان سيف حسن الكمالي[1،2*]
عبدالعزيز عبدالله قائد علي[2،3]
أندرية يفيجنيفيتش زابوليسكي[4]

1باحث في معمل أبحاث السيراميك التقني والمواد النانوية، أستاذ مشارك في قسم "الإلكترونيات الصناعية" بجامعة سوخوي التقنية الحكومية، غوميل، 246029، جمهورية بيلاروسيا، سكوبس: 58547258100، https://orcid.org/0009-0004-3503-1373

2 المنظمة العلمية للبحوث والإبتكارت، الجمهورية اليمنية

3 قسم "الإلكترونيات الصناعية"، باحث مبتديء بجامعة سوخوي التقنية الحكومية، غوميل، 246029، جمهورية بيلاروسيا.

3 طالب دكتوراه في قسم "الإلكترونيات الصناعية" بجامعة سوخوي التقنية الحكومية، غوميل، 246029، جمهورية بيلاروسيا.

†المؤلف المراسل: عبدالعزيز عبدالله قائد علي ، بريد الكتروني : iT.Abdulaziz@Proton.me

ملخص البحث:

تستكشف هذه الدراسة تطور أنظمة التحكم في الوصول (ACS) وتكيفها مع التقنيات الحديثة، مما يعكس التطورات المستمرة في متطلبات الأمن. بتتبع تاريخ التحكم في الوصول، بدءاً من الأقفال الميكانيكية البسيطة في الحضارات القديمة وصولًا إلى التقنيات الذكية المتطورة، نُحلل تأثير ابتكارات مثل القياسات الحيوية وإنترنت الأشياء (IoT) على استراتيجيات إدارة الوصول. يُحدد البحث الاتجاهات والتحديات الرئيسية في أنظمة التحكم في الوصول الحديثة، مُشيراً إلى نقاط ضعف الأمن السيبراني وضرورة تحسين الأطر القانونية. يدمج النموذج المُقترح الأقفال الذكية مع السجلات الصحية الإلكترونية، مما يُتيح لمُقدمي الرعاية الصحية الوصول الآمن إلى بيانات المرضى، مما يُعزز رعاية المرضى وكفاءة العمليات. تُؤكد النتائج على الحاجة إلى التطوير المُستمر ودمج أنظمة التحكم في الوصول الحديثة لمواجهة التحديات الحالية في سياق الرعاية الصحية، لا سيما في مناطق مثل اليمن

الكلمات المفتاحية: أنظمة التحكم في الوصول(ACS) ، المصادقة البيومترية، إنترنت الأشياء(IoT) ، الأمن السيبراني، بيانات المرضى، الإدارة، تقنيات القفل الذكي، السجلات الصحية الالكترونية.(EHR)

ISSN: 2410-7727

I. Introduction

The evolution of Access Control Systems (ACS) reflects the continuous advancement of technology and the changing demands for security. From the emergence of the first systems in ancient civilizations to modern smart technologies, ACS has undergone significant transformations. This paper aims to analyze these changes, focusing on the impact new technologies such as biometrics and the Internet of Things (IoT) have on access management strategies.

The history of access control can be traced back to ancient civilizations, where the need to protect possessions led to the development of mechanical locks [1-15].

- **Ancient Civilizations (circa 2000 B.C.)**: Early access systems comprised simple mechanical locks made of wood and rudimentary mechanisms. These devices were designed primarily to protect property but had limitations, including vulnerability to manipulation.
- **Roman Empire**: Locks evolved with advancements such as spring mechanisms, making them more reliable and difficult to unlock without authorization. Keys became symbols of social status, highlighting the connection between security and societal hierarchy.
- **Middle Ages**: Innovations continued with locks featuring false keyholes, but the issues surrounding unauthorized access remained prevalent. The Middle Ages emphasized the need for more sophisticated solutions.

The Industrial Revolution marked a pivotal shift in lock technology. In 1848, Linus Yale Jr. patented the cylinder lock, which became standard in both residential and commercial buildings. This innovation significantly improved security measures, but mechanical keys were still prone to loss and duplication [1-3].

By the 1970s, advancements in technology brought the first electronic access control systems into play, primarily using magnetic cards. processes: Ems simplified authentication processes; however, they had notable vulnerabilities due to the lack of encryption. Recent history saw the introduction of Radio-Frequency Identification (RFID) technologies in the 1990s, which facilitated faster authentication but faced security flaws in their existing standards [1-6].

The main objective of this research is to analyze the evolution of access control systems, identify key trends, and explore the challenges facing modern systems. This study also aims to illustrate how contemporary technologies, such as biometrics and the Internet of Things (IoT), are reshaping access management practices. By conducting a comparative analysis of current technologies with historical data, we seek to identify potential pathways for the future development of access control systems. Additionally, we aim to develop a system that facilitates access to a patient's medical records for therapists or doctors during appointment registration, utilizing a smart card for secure authentication.

ISSN: 2410-7727

II. Background and Related Work

In [1-5], the authors introduced a review of the historical progression of access control systems highlights the shift from mechanical systems to intelligent platforms that integrate both hardware and software components. Key elements of prior research focused on these systems include the following:

1. **Compatibility**: Legacy systems, such as those based on the Wiegand protocol, fail to support contemporary encryption standards, creating cybersecurity vulnerabilities.
2. **Cyber Threats**: Specific incidents, like the "man-in-the-middle" attacks that threatened RFID systems, highlight the necessity for improved security measures.
3. **Legal Risks**: Conflicts between privacy rights and security requirements, particularly regarding facial recognition technology in the European Union, illustrate the need for nuanced approaches to implementation.

In [5-10], the authors introduced a contemporary trend since the 1920s have featured decentralized identification systems and zero-trust architectures that require multi-factor authentication. The development of quantum-resistant algorithms is anticipated to be vital for future security measures, particularly with the advent of quantum computing. Table 1 below offers a comparative analysis of historical and modern systems.

Table 1 **Comparative analysis of historical and modern systems.**

Parameter	Historical Systems (Pre-2000s)	Modern Systems (Post-2000s)
Technology	Mechanical Locks	RFID, Biometric Systems, IoT
Risk Level	Loss of Keys	Cyber Threats, API Vulnerabilities
Standards	Wiegand Protocol	OSDP, Zero-Trust Architecture
Example Systems	Yale Cylinder Lock	Salto XS4, Brivo
Parameter	Historical Systems (Pre-2000s)	Modern Systems (Post-2000s)

In [11, 12, 13, 18], the authors introduced Contemporary access control systems (ACS) to utilize various technologies that assist organizations in enhancing their security frameworks. Some of the most prevalent technologies include:

1. **Mechanical Systems**: Basic lock systems that, while affordable, have a low security profile.
2. **Electronic Systems**: These systems utilize contactless cards and mobile applications to facilitate entry.

ISSN: 2410-7727

3. **Cloud-Based Systems**: Comprehensive platforms for managing access through the internet.

The following table 2 provides a comprehensive comparison of various access control system (ACS) solutions, highlighting their key features and functionalities. Additionally, it includes specific examples to illustrate each solution, enabling a clearer understanding of the distinctions and applications within the domain of access control[11, 12, 13, 18].

Table 2 **Comparative of ACS Solutions**

Solution Type	Advantages	Disadvantages	Examples
Mechanical Systems	Low Cost	Low Security, Manual Management	Keyguard Lockers
Electronic ACS	Dynamic Management	Vulnerabilities in Protocols, High Licensing Costs	Salto XS4
Cloud-Based ACS	Remote Administration & Analytics	Internet Dependency, Customization Complexity	Brivo, Kisi

The incorporation of emerging technologies into access control systems (ACS) has resulted in the creation of advanced solutions that significantly improve both security and operational efficiency. For example, biometric systems utilize distinct physical characteristics such as fingerprints, iris patterns, and facial recognition for authentication purposes [8, 16, 17].

Biometrics offers several advantages, chief among them being enhanced security, as these systems are significantly harder to replicate than traditional locks. Additionally, they provide users with peace of mind, markedly decreasing the chances of loss or theft. However, despite these benefits, biometric systems encounter criticism and challenges, particularly concerning ethical considerations related to data storage and privacy. Worries about the potential misuse of biometric information and fears surrounding surveillance have sparked ongoing legal discussions regarding regulation and public acceptance [10, 13, 15, 20].

The Internet of Things (IoT) has significantly transformed the functioning of access control systems. IoT devices enable the collection of real-time data, allowing for dynamic adjustments to access permissions based on predefined criteria. For instance, smart locks can provide temporary access to maintenance or emergency personnel while ensuring public safety is not compromised. However, integrating IoT technologies poses challenges such as cybersecurity threats, as these systems are often targeted by attacks, and issues of interoperability, which complicate seamless integration. Recent trends in access control system technology include the following:

ISSN: 2410-7727

multimodal biometrics, which combine facial recognition and fingerprint scanning to enhance reliability and accuracy; decentralized identity (DID) systems, which offer improved privacy and security; zero-trust architectures that necessitate continuous verification of users and devices; and quantum-resistant algorithms designed to safeguard data against potential threats from quantum computing. Table 3 presents an overview of some of these recent trends in ACS technology [1, 9, 11].

Table 3 **summary of several recent trends in access control system (ACS) technology.**

Trend	Description	Potential Impact
Multimodal Biometrics	Combines various biometric methods for enhanced accuracy	Increased user confidence in security
Decentralized Identification	Users manage personal identity data securely	Greater privacy controls
Zero-Trust Architecture	Requires validation at every access attempt	Reduced chances of unauthorized access
Quantum-Resistant Algorithms	Protects against future quantum computing vulnerabilities	Long-term data integrity

III. Methods

i. Architecture of the Proposed Framework

- **Patient Role:** Patients can securely contribute their medical data through a dedicated website that supports the integration of sensors and intelligent devices using digital smart contracts. Currently, electronic health records (EHRs) are fragmented across various healthcare organizations, resulting in inefficiencies in data sharing.
- **Hospital Role:** Hospitals can utilize this framework to manage patient services throughout their care lifecycle effectively. This includes functionalities for uploading and accessing medical information via the online platform.
- **Website Functionality:** The website notifies users of updates to their medical records and allows explicit consent for data sharing. Patients can set time limits on third-party access, maintaining control over which medical records they decide to share.
- **Data Management:** The framework employs a decentralized system that continuously updates health records, ensuring secure storage and rapid retrieval by authorized users. This design minimizes errors, enhances diagnosis and

ISSN: 2410-7727

treatment efficiency, and facilitates personalized care by mitigating miscommunication among healthcare providers.

The proposed framework utilizes a decentralized network architecture that incorporates the Interplanetary File System (IPFS) for data storage. By integrating Ethereum, smart contracts, and IPFS, the system streamlines interactions and establishes a robust health records management infrastructure. Registration on the blockchain is required for all components, except for IPFS storage.

ii. Data Flow and Storage:

- **Hospitals:** Each patient's record is associated with a unique identifier, enabling hospitals to manage record transfers efficiently.
- **Patients:** Patients access their health records through the website and are responsible for executing smart contracts based on the conditions specified during their data submission.
- **Medical Professionals:** Physicians create and maintain patient records, ensuring information integrity. It is imperative to establish policies that uphold patient privacy and security.

iii. Decentralized Architecture: The framework operates on a decentralized model, with encrypted patient data distributed across multiple IPFS nodes. Each record is linked to a unique hash that ensures data integrity. Smart contracts automate essential functions such as data validation and access control, empowering patients to manage consent and actively share their information.

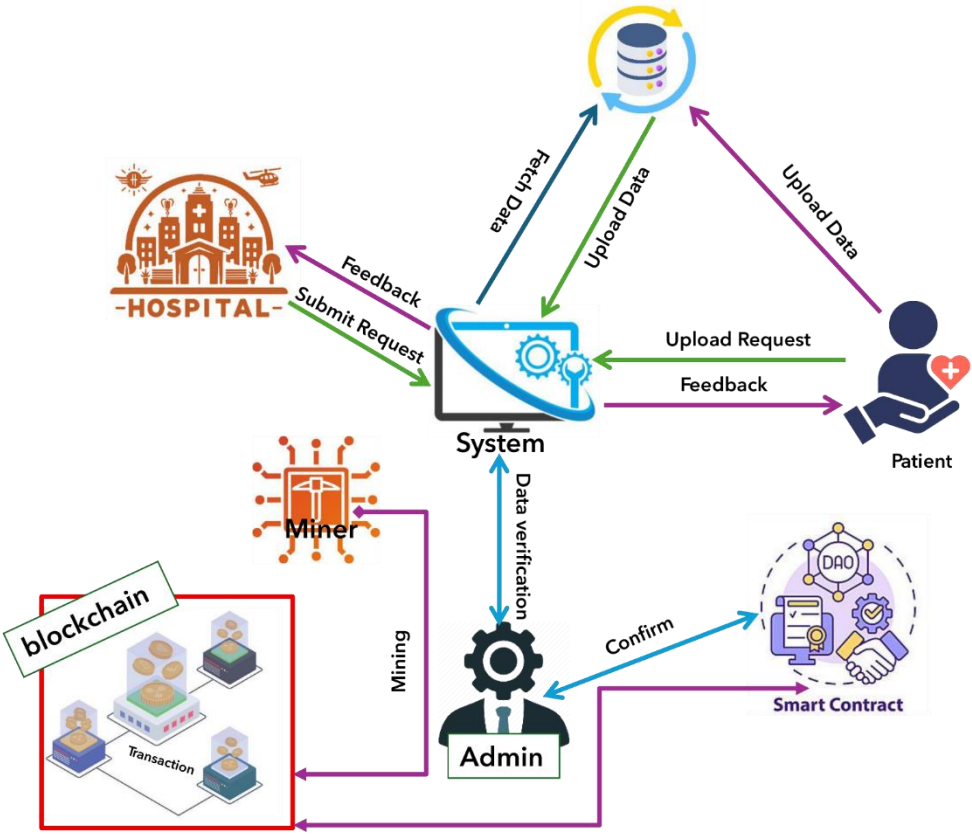
Architecture emphasizes scalability and adaptability for seamless integration with existing electronic health record systems while implementing robust security protocols. Utilizing the Hardhat development environment enhances functionality by facilitating rapid deployment, testing, and debugging smart contracts.

iv. Key Components:

- **Hardhat Platform:** Provides tools for managing the lifecycle of Ethereum applications, optimizing development with features like automated network management and detailed error reporting.
- **Interplanetary File System (IPFS):** Addresses challenges associated with decentralized data storage, reducing data loss risks and enhancing accessibility. Each encrypted data unit is assigned a unique hash for maintaining data integrity.
- **Smart Contracts:** Function as the foundational mechanism of the EHR system, automating key processes and ensuring patient consent is required for accessing medical records.

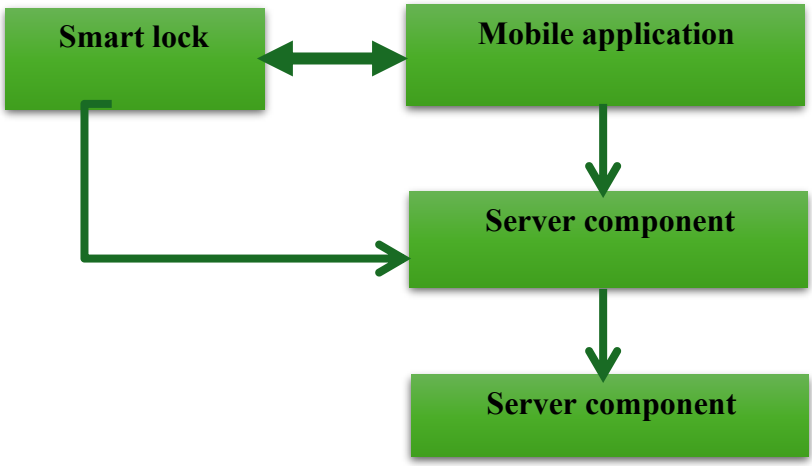
ISSN: 2410-7727

Figure 1 illustrates the diagram of the data structures necessary for storing patient information in the database of the respective hospital.



a) Outline of the Suggested Electronic Health Record (EHR) Framework.

ISSN: 2410-7727



b) A diagram illustrating the data processing mechanism of the smart lock during the input of information.

Figure 1. Proposed Architecture for the Electronic Health Record (EHR) System.

v. **Workflow Summary:** Patients initiate the process by creating an account and uploading their health records. Both patients and hospitals utilize a unique access key for data retrieval. The framework also facilitates innovations such as integrating smart locks that automatically recognize a patient's record through a smart card, enhancing security and workflow efficiency in medical practices.

This cohesive system architecture is specifically designed to improve patient care by integrating various components such as smart locks, data management servers, and mobile applications for patient interaction. The data model captures essential patient information, ensuring secure and efficient management of medical records.

vi. **Key Application Features:**

- **Registration:** Patients register by scanning their appointment cards, allowing the system to accurately link their information with the medical records database.
- **Authentication:** The smart lock unlocks only after the patient's identity is successfully verified via the mobile application.
- **Medical Record Access:** Upon entering the doctor's office, the application quickly downloads the patient's updated information, optimizing the physician's workflow.
- **Notifications:** The system automatically alerts staff to new patient arrivals and allows for updates to medical records after consultations.

ISSN: 2410-7727

The implementation of smart locks and electronic documentation systems aligns with current healthcare trends and the increasing availability of data. Research indicates that electronic medical records (EMRs) significantly improve care quality and enhance patient safety. By integrating an access control system with EMRs, the framework streamlines access processes, reducing the time physicians dedicate to managing patient data, ultimately allowing for more accurate diagnostics. However, several challenges need consideration during the design and deployment of this application:

- **Data Privacy and Security:** Compliance with HIPAA and GDPR regulations must be ensured.
- **Interoperability:** Effective integration with existing systems like EMRs is critical.
- **Technological Infrastructure:** Establishing stable internet connectivity and ensuring reliable equipment operation are essential for optimal functionality.

IV. Results & Discussion

We developed a prototype of a seamless access program utilizing JavaScript frameworks and Solidity Coverage, designed for both patients and doctors. This program serves as a comprehensive link to patient information, including health status, treatment details, and the treatment physician's credentials.

Security is a top priority; access is strictly controlled, ensuring that only authorized individuals can view sensitive information. Patients can register from home or online, and their smart cards can be utilized upon arrival at the hospital. This triggers an alert to the doctor regarding the patient's presence.

Once in the examination room, the patient's medical record, securely stored in the hospital database, opens automatically, providing the doctor with immediate access to essential information. The implementation details are as follows:

1. Command code specific to the data-receiving server

```
// server.js
const express = require('express');
const mongoose = require('mongoose');
const bodyParser = require('body-parser');
const cors = require('cors');
const app = express();

// ===== Middleware =====
app.use(cors());
app.use(bodyParser.json());

// ===== MongoDB Connection =====
```

ISSN: 2410-7727

```
   mongoose.connect('mongodb://localhost:27017/medicalDB
', {
       useNewUrlParser: true,
       useUnifiedTopology: true,
   })
   .then(() => console.log("MongoDB connected"))
   .catch(err   =>   console.error("MongoDB   connection
error:", err));

   // ===== Patient Schema =====
   const patientSchema = new mongoose.Schema({
       name: { type: String, required: true },
       birthdate: { type: Date, required: true },
       medicalHistory: { type: String, default: "" },
       cardID: { type: String, unique: true, required:
true }
   });

   // ===== Patient Model =====
   const     Patient     =     mongoose.model('Patient',
patientSchema);

   // ===== API Endpoints =====

   // Register a patient
   app.post('/register', async (req, res) => {
       try {
           const   {   name,   birthdate,   medicalHistory,
cardID } = req.body;
           const   existing   =   await   Patient.findOne({
cardID });
           if (existing) {
               return    res.status(400).send("Card    ID
already exists");
           }
           const patient = new Patient({ name, birthdate,
medicalHistory, cardID });
           await patient.save();
           res.status(201).send('Patient      registered
successfully');
       } catch (err) {
           console.error(err);  // Log the error details
```

ISSN: 2410-7727

```
            res.status(500).send("Server error");
        }
    });

    // Fetch patient by card ID
    app.get('/patient/:cardID', async (req, res) => {
        try {
            const patient = await Patient.findOne({
cardID: req.params.cardID });
            if (!patient) return
res.status(404).send('Patient not found');
            res.json(patient);
        } catch (err) {
            console.error(err);  // Log the error details
            res.status(500).send("Server error");
        }
    });

    // ===== Start Server =====
    const PORT = process.env.PORT || 5000;
    app.listen(PORT, () => console.log(`Server running on
port ${PORT}`));
```

2. UI Command Code

```
    // App.js
    import React, { useState } from 'react';
    import { View, TextInput, Button, Text, StyleSheet }
from 'react-native';
    import axios from 'axios';

    export default function App() {
        const [cardID, setCardID] = useState('');
        const [patientData, setPatientData] =
useState(null);

        const handleFetchPatient = async () => {
            if (!cardID.trim()) {
                alert("Please enter a Card ID");
                return;
            }
            try {
```

ISSN: 2410-7727

```
                const response = await
axios.get(`http://YOUR_SERVER_IP:5000/patient/${cardID}
`);
                setPatientData(response.data);
            } catch (error) {
                alert("Patient not found");
                setPatientData(null);
            }
        };

        return (
            <View style={styles.container}>
                <TextInput
                    placeholder="Enter Card ID"
                    value={cardID}
                    onChangeText={setCardID}
                    style={styles.input}
                />
                <Button title="Fetch Patient"
onPress={handleFetchPatient} />
                {patientData && (
                    <View style={styles.result}>
                        <Text>Name:
{patientData.name}</Text>
                        <Text>Birthdate: {new
Date(patientData.birthdate).toLocaleDateString()}</Text
>
                        <Text>Medical History:
{patientData.medicalHistory}</Text>
                    </View>
                )}
            </View>
        );
    }

    const styles = StyleSheet.create({
        container: {
            padding: 20,
            marginTop: 50,
        },
        input: {
            height: 40,
```

ISSN: 2410-7727

```
            borderColor: 'gray',
            borderWidth: 1,
            paddingHorizontal: 10,
            marginBottom: 20,
        },
        result: {
            marginTop: 20,
            backgroundColor: "#f2f2f2",
            padding: 15,
            borderRadius: 10,
        },
    });
```

Once the code has been implemented, the user will encounter one of the available interfaces. This interface enables users to input their information after registering as a patient at the hospital. In the future, they can access their data either by manually entering it, using a fingerprint or iris scan from home, or by utilizing the electronic patient card provided by the hospital. The relevant interfaces are illustrated in Figure 2.

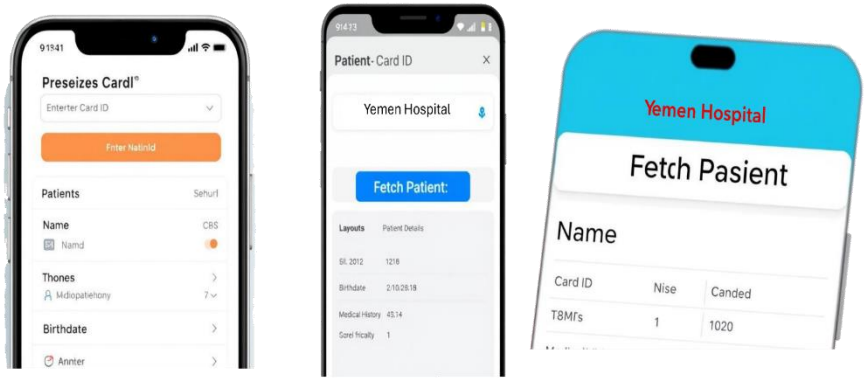


Figure 2. Screenshot of the interface displays to the user when using the phone recording application

This interface serves as a preliminary and initial version of the program, which can be modified to achieve its final form. We will carry out further studies to refine the interfaces and enhance the program's accuracy, aiming to bolster the security of the entered data. The information will be encrypted to prevent unauthorized access.

ISSN: 2410-7727

V. Conclusions

Creating a smart lock application for a doctor's clinic, which incorporates appointment card registration, marks a significant advancement in the automation of healthcare processes. This solution not only streamlines access to clinics but also enhances staff efficiency and improves patient care quality. Modern Access Control Systems (ACS) are intricate frameworks that combine hardware, software, and networking elements to provide targeted resource access. As technology evolves, a multidisciplinary approach is essential, integrating encryption, data analysis, and legal considerations to safeguard information and resources effectively.

The ongoing evolution of ACS is crucial in addressing complex challenges, particularly considering rising cybersecurity threats and the increasing importance of personal data protection. Understanding the historical context and current implementations of ACS is vital for successfully designing systems that meet contemporary requirements. Historically, ACS has transformed from mechanical locks to sophisticated smart platforms that integrate hardware, software, and organizational structures. Today, it is imperative to consider not only technological aspects but also legal, ethical, and data protection issues.

Given the challenges presented by today's technological landscape, there is a clear and growing need for the enhancement and adaptation of access control systems.

The development of these systems not only bolsters security but also improves overall resource management efficiency, positioning them as critical components of both business and societal infrastructure. This underscores the necessity for ongoing research and development in this field.

The proposed architecture and coding model lay the groundwork for an application that allows for efficient and secure patient registration via a smart lock at the doctor's clinic. Future enhancements could introduce functionalities such as notifications for doctors regarding new patients and streamlined updates to medical records.

In the context of Yemen, implementing such systems will simplify processes for patients and healthcare providers during routine checkups, reducing the risk of chronic diseases and facilitating preventive measures. Additionally, it will ease appointment scheduling at clinics, mitigate overcrowding, and lower the likelihood of infectious disease spread. The registration system could also integrate a dedicated hotline for emergencies, promptly alerting the hospital when activated by a patient.

ISSN: 2410-7727

VI. Acknowledgements.

The work was carried out within the framework of task 2.2.6 of the state research program “Convergence-2025” (subprogram “Microcosm, plasma and the Universe”), funded from the republican budget for state research programs for 2021–2025 in the Republic of Belarus. All experiments were prepared in the Laboratory of Technical Ceramics and Nanomaterials, Sukhoi State Technical University in Gomel, Gomel, Belarus.

ISSN: 2410-7727

VII. References

1. Clarke, R. Smart Lock Systems: Design and Security Challenges / R. Clarke // IEEE Transactions on Dependable and Secure Computing. – 2013. – Vol. 10, No. 4. – P. 345–352.
2. GOST R 51241-2008. Access control and management systems and means. Classification. General technical requirements. – Moscow: Standartinform, 2008. – 18 p. (in Russian).
3. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. – Gaithersburg, MD: NIST, 2022. – 96 p.
4. SALTO Systems. Case Study: SALTO KS Keyscript в образовательных учреждениях. – 2021. – URL: https://www.saltosystems.com/en/solutions/education/ (date of access: 01.06.2025).
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva: ISO, 2022. – 44 p.
6. Verizon. Data Breach Investigations Report / Verizon DBIR. – 2023. – URL: https://www.verizon.com/business/resources/reports/dbir/ (date of access: 01.06.2025).
7. Daugman, J. How Iris Recognition Works / J. Daugman // IEEE Transactions on Circuits and Systems for Video Technology. – 2004. – Vol. 14, No. 1. – P. 21–30.
8. J. Gui, Z. Sun, Y. Wen, D. Tao and J. Ye, "A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications," in IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 4, pp. 3313-3332, 1 April 2023, doi: 10.1109/TKDE.2021.3130191.
9. N. Farhadighalati, L. A. Estrada-Jimenez, S. Nikghadam-Hojjati and J. Barata, "A Systematic Review of Access Control Models: Background, Existing Research, and Challenges," in IEEE Access, vol. 13, pp. 17777-17806, 2025, doi: 10.1109/ACCESS.2025.3533145.
10. Alzahrani, B., Alsolami, F. (2019). Biometric System: Security Challenges and Solutions. In: Latifi, S. (eds) 16th International Conference on Information Technology-New Generations (ITNG 2019). Advances in Intelligent Systems and Computing, vol 800. Springer, Cham. https://doi.org/10.1007/978-3-030-14070-0_17
11. Ali, L. A. M. The impact on governments of the sharp rise in tax fraud utilizing artificial intelligence [Electronic resource] / L. A. M. Ali, N. F. S. H. AL-Kamali; scientific supervisor M. F. S. H. AL-Kamali // E.R.A - Modern science: electronics, robotics, automation: materials of the I International. scientific-technical Conf., students, graduate students and young scientists, Gomel, February 29. 2024 / Gomel. state tech. University named after P. O. Sukhoi [and

ISSN: 2410-7727

others]; under general ed. A. A. Boika. – Gomel: GGTU, 2024. – pp. 158–159 .
12. Al-Aimiri, M. A. M. K. Designing Website Interfaces Using Artificial Intelligence Tools [Electronic resource] / M. A. M. K. Al-Aimiri; scientific supervisor M. F. S. AL-Kamali // MITRO 2023 – Mechanical Engineering. Innovations. Technologies. Robotics: abstracts of reports. scientific and technical. conf. students and young scientists / Gomel, December 6, 2023 – Gomel: GSTU, 2023. – P. 140.
13. Das, R. (2016). Adopting Biometric Technology: Challenges and Solutions (1st ed.). Routledge. https://doi.org/10.1201/9781315369945
14. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. Sensors 2023, 23, 1805. https://doi.org/10.3390/s23041805
15. Al-Ameri, O. A. S. M. Establishing an open-access program connecting all medical facilities via unique accounts for each beneficiary in Yemen / O. A. S. M. Al-Ameri; scientific supervisor M. F. S. H. AL-Kamali // I International Youth Scientific and Cultural Forum of Students, Master's Degree Students, Postgraduate Students and Young Scientists [Electronic resource]: collection of materials, Gomel, March 5-7, 2024 / Ministry of Education of the Republic of Belarus; Gomel State Technical University named after P. O. Sukhoi; Taiz University; Scientific Organization for Research and Innovation; edited by A. A. Boika. – Gomel: GSTU, 2024. – P. 46.
16. Ross Anderson, "Distributed Systems," in Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2020, pp.243-273, doi: 10.1002/9781119644682.ch7.
17. AL-Aimiri, M. A. M. K. Streamlining factory operations: designing an effective manufacturing management program / M. A. M. K. AL-Aimiri, M. F. S. H. AL-Kamali // Innovative machine tool building, technologies and tools: proc. I Intern. scientific-practical. conf., Gomel, November 30, 2023 / Ministry of Industry of the Republic of Belarus [et al.]; under the general editorship of M. I. Mikhailov. - Gomel: GSTU, 2024. - P. 105-106.
18. Sayali Renuse, Parikshit N. Mahalle, Gitanjali Rahul Shinde, and Nilesh P. Sable. 2024. A Comparative Study of Access Control Models for Ubiquitous Computing Systems. In Proceedings of the 5th International Conference on Information Management & Machine Intelligence (ICIMMI '23). Association for Computing Machinery, New York, NY, USA, Article 78, 1–6. https://doi.org/10.1145/3647444.3647905
19. Oladoyinbo, T. O., Oladoyinbo, O. B., & Akinkunmi, A. I. (2024). The Importance of Data Encryption Algorithms in Data Security. IOSR Journal of Mobile Computing & Application (IOSR-JMCA), 11(2), 10-16. e-ISSN: 2394-0050, p-ISSN: 2394-0042. Retrieved from www.iosrjournals.org

ISSN: 2410-7727

20. Ibrahim, R. M., El-afifi, M. I., & El Kelany, M. M. (2023). Trends in Biometric Authentication: A Review. Nile Journal of Communication and Computer Science, 6(1), 63-75. DOI: 10.21608/njccs.2023.220975.1015. Nile Higher Institute for Engineering and Technology.
21. Alhammadi OAS, Mohamed HI, Musa SS, Ahmed MM, Lemma MA, Joselyne U, et al. Advancing digital health in Yemen: challenges, opportunities, and way forward. Explor Digit Health Technol. 2024;2:369–86. https://doi.org/10.37349/edht.2024.00035

ISSN: 2410-7727

مجلـــة الأندلـــس للعلـــوم الإنسانيـــة والاجتماعيـــة
مجلـــة دوليـــة شهـريـــة علميـــة محكمـــة
الترقيـــم الدولي الإلكتروني : ISSN : 2410– 521X
الترقيـــم الدولـــي الورقـــي :ISSN :2410– 1818
البريد الإلكتروني : journal@andalusuniv.net

المجلـــة مفهرســـة فـــي المواقـــع الآتيـــة :

العام	2021	2022	2023	2024	2025
معامل أرسيف	0.2692	0.1954	0.3759	0.3068	0.5978
معامل التأثير العربي	1.60	1.73	1.25	1.55	1.81