The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

Quantum-Resistant IoT Smart Locking Systems for Enhanced Security

B.Pavitra1 , D.Narendar Singh2, R.Nagaswetha3 1,2,3School of Computing, Dept of ECE, Anurag University, Hyderabad,Telangana-India Corresponding Author *: pavitraece@anurag.edu.in

క్వాంటం-రెసిస్టెంట్ ఐఓటీ స్మార్ట్ లాకింగ్ వ్యవస్థలు కోసం మెరుగుపరచబడింది భద్రత

బి. పవిత్ర [1] , డి.నరేందర్ సింగ్ [2] , ఆర్. నాగస్వేత [3]
[1,2,3] పాఠశాల యొక్క కంప్యూటింగ్, విభాగం యొక్క ఇసిఇ, అనురాగ్ విశ్వవిద్యాలయం, హైదరాబాద్,

తెలంగాణ-భారతదేశం సంబంధిత రచయిత *: pavitraece@anurag.edu.in

వియుక్త

నేటి ప్రపంచీకరణ ప్రపంచంలో భద్రత మరింత ప్రాముఖ్యతను సంతరించుకుంది. యాంత్రిక తాళాలు సరళమైనవి కు ఓవర్‌రైడ్ మరియు అందించండి కనిష్ట భద్రత వ్యతిరేకంగా సమకాలీన పద్ధతులు యొక్క చొరబాటు. IoT- ఆధారిత స్మార్ట్ డోర్ లాక్‌ల ఉనికి నివాస, వాణిజ్య మరియు పారిశ్రామిక అనువర్తనాలకు నమ్మకమైన, ఉపయోగించడానికి సులభమైన పరిష్కారాలను అందిస్తుంది. ఈ పత్రం మెరుగైన స్మార్ట్ లాకింగ్ వ్యవస్థను అందిస్తుంది, వీటిని ఉపయోగిస్తుంది ఆర్డునో యుఎన్ఓ, పొందుపరచబడింది ఐఓటీ పరికరాలు, మరియు ఉద్భవిస్తున్న భద్రత నమూనాలు ఇష్టం క్వాంటం-రెసిస్టెంట్ క్రిప్టోగ్రఫీ మరియు మెషిన్-లెర్నింగ్-ఆధారిత ప్రామాణీకరణ. క్వాంటం-రెసిస్టెంట్ అమలుతో క్రిప్టోగ్రాఫిక్ అల్గోరిథంలు మరియు రియల్-టైమ్ మేఘం కనెక్టివిటీ, ది వ్యవస్థ ప్రతిపాదిత భవిష్యత్తు-రుజువు మరియు స్కేలబుల్ భద్రతను అందిస్తుంది.

కీలకపదాలు:
స్మార్ట్ లాకింగ్ వ్యవస్థ, క్వాంటం కంప్యూటింగ్, ఐఓటీ భద్రత, పోస్ట్-క్వాంటం క్రిప్టోగ్రఫీ, MQTT / వై-ఫై / బిఎల్ఇ కమ్యూనికేషన్

1.పరిచయం

యాక్సెస్ నియంత్రణ రూపాలు ది పునాది కోసం భౌతిక మరియు సైబర్ భద్రత. టెక్నాలజీ కలిగి నుండి ముందుకు సాగింది యాంత్రిక కీలు కు ఎలక్ట్రానిక్ తాళాలు తో RFID, ఓటీపీ, మరియు బయోమెట్రిక్ ధృవీకరణ. తలుపు లాక్‌లు ఇప్పుడు మొబైల్ అప్లికేషన్‌లు, హోమ్ అసిస్టెంట్‌లు మరియు రిమోట్‌కు

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

మద్దతు ఇచ్చే క్లౌడ్ ఆధారిత పరికరాలకు కనెక్ట్ చేయబడ్డాయి పర్యవేక్షణ మరియు నియంత్రణ IoT పరికరాలు విస్తరించడం కొనసాగిస్తున్నందున. ఈ IoT పరికరాలు ఇప్పుడు ఎక్కువగా ఉన్నాయి దుర్బలమైన కు సైబర్ దాడులు మరియు అందుకే అవసరం ఉన్నత స్థాయి ఎన్క్రిప్షన్ మరియు అధునాతన అసాధారణ గుర్తింపు. క్వాంటం కంప్యూటింగ్ పురోగతులు సాంప్రదాయాన్ని ప్రమాదంలో పడేస్తున్నాయి ఎన్క్రిప్షన్ క్వాంటం తో పద్ధతులు నిరోధక క్రిప్టోగ్రఫీ (ఉదా., లాటిస్-ఆధారిత క్రిప్టోగ్రఫీ) పరిశోధనలో ఉంది. IoT-సామర్థ్యం గల స్మార్ట్ లాక్‌లలో అటువంటి అల్గోరిథంల విస్తరణ భవిష్యత్తు-రుజువు భద్రత రాబోయే క్వాంటం-ఆధారిత ముప్పులకు వ్యతిరేకంగా. AI -ఆధారిత విశ్లేషణలు క్రమరహితాలను నిజ-సమయంలో గుర్తించడం ద్వారా విశ్వసనీయతను మరింత మెరుగుపరుస్తాయి. యాక్సెస్ నమూనాలు మరియు క్రూరమైన శక్తి ప్రయత్నాలు. ఇది కాగితం సూచిస్తుంది ఒక ఆర్డునో యుఎన్ఓ మరియు ఐఓటీ హార్డ్‌వేర్-అమలు చేయబడినది బలోపేతం చేయబడింది తలుపు లాక్ తో ది ఐచ్ఛికం లక్షణం యొక్క ఉపయోగించి క్వాంటం-సేఫ్ ఎన్‌క్రిప్షన్ మరియు క్లౌడ్‌లో పర్యవేక్షణ.

2. సాహిత్యం సర్వే

[1] అక్షయ కృష్ణదాస్ భట్ మరియు అల్. ది ఉద్భవం యొక్క తెలివైన తలుపు లాక్ టెక్నాలజీ ఉంది ఒక పూర్వగామి కు వేగంగా అనుసంధానం యొక్క ఎలక్ట్రానిక్స్, ఐఓటీ, మరియు సైబర్ భద్రత. ప్రారంభ పరిశోధనలు, కోసం ఉదాహరణకు, ద్వారా భట్ మరియు ఇతరులు, Arduino బోర్డుల ఆధారంగా పాస్‌వర్డ్-రక్షిత తలుపులను అభివృద్ధి చేశారు, తక్కువ ధర మైక్రోకంట్రోలర్‌లు ప్రామాణిక మెకానికల్ తాళాల కంటే మెరుగైన గృహ భద్రతను అందించగలవని చూపించారు. [2] ప్రభాకర్ మరియు ఇతరులు ఆర్థికంగా ఉండే Arduino UNO- ఆధారిత తాళాలను సూచించడం ద్వారా దీనిని ఒక అడుగు ముందుకు వేశారు. మరియు సరళమైనది కు ఇన్‌స్టాల్ చేయండి లో కార్యాలయాలు, ఇళ్ళు, మరియు పాఠశాలలు. కుమార్ మరియు అల్. సూచించబడింది బ్లూటూత్ ఆధారిత లాక్‌లు, ఇక్కడ బ్లూటూత్ స్మార్ట్‌ఫోన్‌లు మరియు ఆర్డుయినో మధ్య కమ్యూనికేషన్ వంతెనగా పనిచేసింది, మొబైల్-యాక్సెస్ నియంత్రణ సామర్థ్యాన్ని ప్రదర్శిస్తుంది. ఈవెంట్‌లను లాగ్ చేయడానికి మరియు స్థితిని ధృవీకరించడానికి క్లౌడ్ డాష్‌బోర్డ్‌లతో డోర్ లాక్‌లను సమకాలీకరించడానికి Wi-Fi మాడ్యూల్స్ ద్వారా సుదూర కనెక్టివిటీని మరిన్ని పరిణామాలు చూపించాయి. RFID ధృవీకరణ అనేది విస్తృతమైన కాంటాక్ట్‌లెస్ ప్రత్యామ్నాయం, మరియు వేలిముద్ర మరియు ముఖ గుర్తింపు సెన్సార్లు ఆఫర్ మెరుగుపడింది, బహుళ-కారకం భద్రత. [3] MQTT మరియు మేటర్ స్టాండర్డ్ వంటి తక్కువ-శక్తి IoT ప్రోటోకాల్‌లు మరింత సరైన కమ్యూనికేషన్‌లు మరియు పరికర ఇంటర్‌ఆపరేబిలిటీని అనుమతిస్తాయి మరియు పెద్ద స్మార్ట్-హోమ్ కేంద్రంలో స్మార్ట్ లాక్‌లను ఉంచుతాయి. వ్యవస్థలు. శక్తి సామర్థ్యం ఉంది కూడా లో దృష్టి, ఉదా, కోసం బ్యాటరీతో నడిచేది తాళాలు, ఫలితంగా లో తక్కువ శక్తి హార్డ్వేర్ మరియు పంట కోత శక్తి నుండి సూర్యకాంతి లేదా గతిశాస్త్రం మూలాలు. అదే సమయంలో, బ్రూట్-ఫోర్స్ దాడులను లేదా లాగిన్‌ల అసాధారణ నమూనాలను గుర్తించడానికి AI -

CC BY

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

ఆధారిత విశ్లేషణలను ఉపయోగించారు, అక్రమ యాక్సెస్‌కు వ్యతిరేకంగా ప్రతిఘటనను పెంచారు. ఇటీవలి ప్రయత్నాలు రాబోయే క్వాంటంపై దృష్టి సారించాయి క్లాసికల్ ఎన్క్రిప్షన్ పద్ధతులను బద్దలు కొట్టగల కంప్యూటర్ ముప్పు. [4] ఎంబెడెడ్ హార్డ్‌వేర్‌కు మద్దతు ఇవ్వడానికి లాటిస్-ఆధారిత ఎన్‌క్రిప్షన్ మరియు హాష్-ఆధారిత సంతకాలుగా పోస్ట్-క్వాంటం క్రిప్టోగ్రఫీని ప్రదర్శించారు. తో చిన్నది జాప్యం, మరియు NIST లు ప్రమాణాలు గైడ్ లో 2024 నియంత్రణ ది ఎంపిక యొక్క క్వాంటం-నిరోధకత పథకాలు. అక్కడ ఉన్నాయి కూడా వ్యాసాలు దర్యాప్తు చేయడం ది అప్లికేషన్ యొక్క క్వాంటం కీ అల్ట్రా-హై-సెక్యూరిటీ వాతావరణాలలో పంపిణీ. పిన్‌లు, బయోమెట్రిక్స్, RFID మరియు అనామలీలను కలుపుకొని హైబ్రిడ్ వ్యవస్థలు గుర్తింపు ప్రదర్శించు ఒక బహుళ పొరలు కలిగిన రక్షణ స్థానం, మరియు చొరబాటు సెన్సార్లు మరియు ట్యాంపర్-ప్రూఫ్ ఎన్‌కేస్‌మెంట్‌లు అదనపు శారీరక బలాన్ని అందిస్తాయి. ప్రామాణీకరణను తగ్గించడానికి ఎడ్జ్ కంప్యూటింగ్ సూచించబడింది జాప్యం ద్వారా స్థానిక ఆధారాలు ప్రాసెసింగ్, మరియు స్థిరమైన డిజైన్ ఉంది గురిపెట్టిన వద్ద పొడవైన బ్యాటరీ జీవితం మరియు శక్తి పంట కోత. వినియోగం పరీక్ష తుది-వినియోగదారు స్వీకరణను పరిశీలిస్తుంది యొక్క బయోమెట్రిక్ మరియు క్వాంటం-సురక్షిత లాక్‌లు మరియు ఆ పరిచయాన్ని కనుగొంటాయి మరియు అభిప్రాయం స్వీకరణను మెరుగుపరుస్తాయి. మొత్తంగా, ఈ సేకరణ యొక్క పరిశోధన జాడలు అభివృద్ధి నుండి ప్రాథమిక కీప్యాడ్ తాళాలు కు అధునాతనమైన, ఎన్‌క్రిప్ట్ చేయబడింది IoT, AI మరియు క్వాంటం-రెసిస్టెంట్ క్రిప్టో యొక్క పరికరాల మాషప్‌లు. ఈ పని సమగ్రపరచడం ద్వారా ఈ ఫలితాలను విస్తరిస్తుంది. ఆర్డునో, ఐఓటీ నెట్‌వర్కింగ్, అసాధారణత గుర్తింపు, మరియు పోస్ట్-క్వాంటమ్ ఎన్క్రిప్షన్ కు సృష్టించు భవిష్యత్తుకు అనుకూలమైన, స్కేలబుల్ భద్రతా పరిష్కారం.

3. పద్ధతి

తెలివైన వ్యక్తి కోసం వ్యూహాన్ని రూపొందించండి తదుపరి లాకింగ్ వ్యవస్థ తరం ఏకీకరణ చుట్టూ కేంద్రీకృతమై ఉంది యొక్క ఒక ఆర్డునో యుఎన్ఓ నియంత్రిక తో ఐఓటీ, క్వాంటం-నిరోధకత క్రిప్టోగ్రఫీ, మరియు యాక్సెస్ చేయగల యాక్సెస్ విధానాలు. ప్రారంభించండి Arduino UNO ని నిర్వచించడం నియంత్రించే మాస్టర్ ప్రాసెసింగ్ యూనిట్ అన్నీ ఉపవ్యవస్థలు, అటువంటివి గా ప్రామాణీకరణ, మోటార్ డ్రైవ్ మరియు కమ్యూనికేషన్ డేటా యొక్క. అ వినియోగదారు రకాలు ఒక పాస్‌వర్డ్ లేదా బయోమెట్రిక్ సమాచారం ఉపయోగించి ఒక ఇన్‌పుట్ ఇంటర్‌ఫేస్, అంటే గా ఒక సాదా 4×4 కీప్యాడ్, కెపాసిటివ్ తాకండి స్క్రీన్, లేదా అధునాతన బయోమెట్రిక్ సెన్సార్లు ఇష్టం వేలిముద్ర లేదా ముఖ గుర్తింపు రీడర్లు. అటువంటి ఇన్‌పుట్‌లను స్థానికంగా తనిఖీ చేస్తారు నిల్వ చేసిన ఆధారాలకు వ్యతిరేకంగా Arduino లేదా సురక్షితమైన ద్వారా రిమోట్‌గా ప్రామాణీకరించబడింది Wi-Fi ద్వారా క్లౌడ్ సర్వర్ లేదా బ్లూటూత్ తక్కువ శక్తి (BLE). కు తప్పించు ఆధారాలు దొంగతనం లేదా వినడం,

CC BY

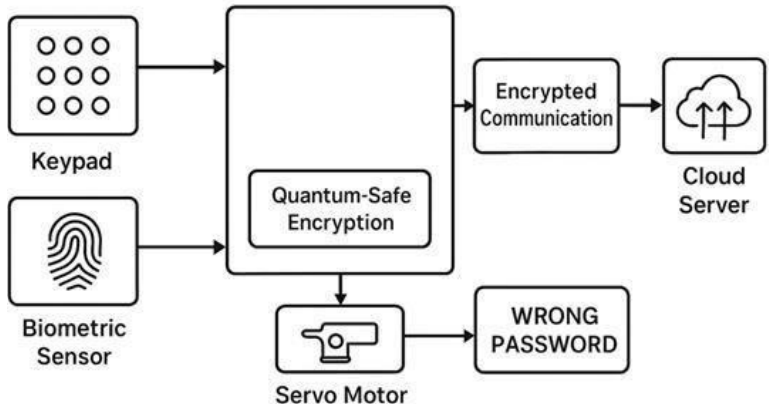
The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

కమ్యూనికేషన్ మధ్య ది పరికరం మరియు క్లౌడ్ సేవలు ఉంది రవాణా పొర భద్రత (టిఎల్ఎస్) ఎన్క్రిప్ట్ చేయబడింది లేదా, ఎక్కడ అవసరమైన, లాటిస్-ఆధారిత లేదా హాష్-ఆధారిత ఎన్క్రిప్షన్ లైబ్రరీల వంటి క్వాంటం-నిరోధక అల్గారిథమ్‌లు. విజయవంతమైన ప్రామాణీకరణ తర్వాత, ఆర్డుయినో పంపుతుంది ది నియంత్రణ a కి సంకేతాలు సర్వో మోటార్ ఆపరేటింగ్ లాక్ మెకానిజం కు తిప్పండి గొళ్ళెం అన్‌లాక్ చేయండి కోసం ఒక విరామ వ్యవధి. ఆన్ వైఫల్యం ప్రమాణీకరణ, ది వ్యవస్థ అంటే లాక్ చేయబడింది, మరియు అభిప్రాయం లో నిజమైన సమయం నుండి ఒక ఎల్‌సిడి లేదా OLED తెలుగు in లో ప్రదర్శన తెలియజేస్తుంది ది వినియోగదారు యొక్క "తప్పు పాస్‌వర్డ్" లేదా "యాక్సెస్ నిరాకరించబడింది." పునరావృతమైతే వైఫల్యాలు, అలారం అందింది నిర్వాహక స్మార్ట్‌ఫోన్ ద్వారా లేదా మేఘం డాష్‌బోర్డ్, మరియు వ్యవస్థ చెయ్యవచ్చు ఉండండి సెట్ కు ప్రవేశించు లాకౌట్ మోడ్ కు క్రూరత్వాన్ని నిరోధించండి దాడులు. కోసం మద్దతు ఇవ్వడం ఐఓటీ కార్యాచరణ, ది వ్యవస్థ బొమ్మ 1, ఉంది ఒక వై-ఫై మాడ్యూల్ (ఉదా, ESP8266/ESP32) లేదా BLE హార్డ్‌వేర్ అది మద్దతు ఇస్తుంది ఈవెంట్ లాగింగ్, రిమోట్ అన్‌లాకింగ్ మరియు ఫర్మ్‌వేర్ నవీకరణలు. MQTT లేదా HTTPS వంటి తేలికపాటి ప్రోటోకాల్‌లను ఉపయోగించి సమాచారం తెలియజేయబడుతుంది, అది మద్దతు కోసం స్మార్ట్-హోమ్ హబ్‌లు ఆధారిత ఆన్ ది విషయం ప్రామాణికం ఉంది హామీ ఇవ్వబడింది. AI -ఆధారిత అసాధారణత గుర్తింపు అల్గోరిథంలు చెయ్యవచ్చు ఉండండి అమలు చేయబడింది స్థానికంగా లేదా లో ది మేఘం, పర్యవేక్షణ నమూనాలు యొక్క యాక్సెస్ మరియు మార్కింగ్ అనుమానాస్పదమైన కార్యాచరణ లో నిజమైన సమయం. శక్తి నిర్వహణ ఉంది తీసుకున్న జాగ్రత్త యొక్క ద్వారా ది ఉపయోగం యొక్క తక్కువ వినియోగ హార్డ్‌వేర్, స్లీప్ మోడ్‌లు మరియు ప్రత్యామ్నాయ పునరుత్పాదక శక్తి రూపంలో చిన్న సౌర ఫలకాలు లేదా గతిశాస్త్రం ఛార్జింగ్. ది సర్వో మోటారు ఉంది కూడా PID-ట్యూన్ చేయబడింది కు పరుగు సజావుగా మరియు స్థిరంగా మరియు విద్యుత్ వినియోగాన్ని తగ్గించండి. అంతా ఆర్డునో నుండి మోటారు, కీప్యాడ్, మరియు డిస్ప్లే లోపల ఉంది ఒక మోసపూరితమైన కేసు తో చొరబాటు డిటెక్టర్లు అది ధ్వని అలారాలు ఎప్పుడు ది కేసింగ్ ఉంది తెరవబడింది. సిస్టమ్ మాడ్యులర్ అప్‌గ్రేడ్‌లకు మద్దతు ఇచ్చే సాఫ్ట్‌వేర్ ఆర్కిటెక్చర్‌ను నిర్వహిస్తుంది, తద్వారా RFID కార్డులు, NFC మొబైల్ ఫోన్‌లు లేదా అల్ట్రా-సెక్యూర్ సెంటర్‌ల కోసం క్వాంటం కీ పంపిణీ వంటి కొత్త ప్రామాణీకరణ పద్ధతులను జోడించవచ్చు. డెవలపర్లు. యాక్సెస్ లాగ్‌లు మరియు పనితీరు కొలమానాలు స్థానిక నిల్వలో ఉంచబడతాయి మరియు విశ్వసనీయత కోసం క్లౌడ్ నిల్వకు సమకాలీకరించబడతాయి. నెట్‌వర్క్‌లో ఉన్నప్పుడు కూడా అంతరాయాలు. ఇది బహుళ-స్థాయి భద్రతా వ్యూహాన్ని కలిగి ఉంది, స్థానికంగా ఎన్క్రిప్టెడ్ క్లౌడ్‌తో ప్రామాణీకరణ పెంచబడింది-

CC BY

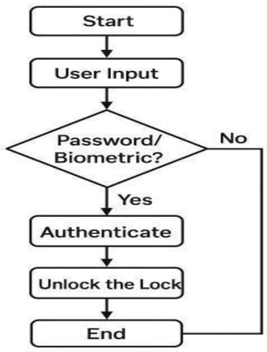
The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

ఆధారిత ధృవీకరణ మరియు సాధారణ ఫర్మ్‌వేర్ నవీకరణలు సంతకం చేయబడింది తో పోస్ట్-క్వాంటమ్ క్రిప్టోగ్రాఫిక్ కీలు అనధికార కోడ్ ఇంజెక్షన్ నుండి రక్షించడానికి .



చిత్రం 1: క్వాంటం-రెసిస్టెంట్ ఆధారిత ఐఓటీ స్మార్ట్ లాకింగ్ వ్యవస్థలు

ప్రోటోటైప్ పరీక్షలో ప్రామాణీకరణ రేటు, ఎన్‌క్రిప్షన్ పెనాల్టీ, సర్వో ప్రతిస్పందన సమయం మరియు సాధారణ విద్యుత్ వినియోగం యొక్క అంచనా కూడా ఉంటుంది. గృహ మరియు కార్యాలయ వాతావరణ వినియోగ పరిస్థితులు. ఒత్తిడి పరీక్షలలో పదేపదే విఫలమైన లాగిన్ ప్రయత్నాలను అనుకరించడం మరియు లాకౌట్ మరియు హెచ్చరిక లక్షణాలను పరీక్షించడం వంటివి ఉంటాయి. ఈ విధానం ద్వారా, సూచించబడిన స్మార్ట్ లాక్ IoT, AI మరియు క్వాంటం-రెసిస్టెంట్ క్రిప్టోగ్రఫీని ఉపయోగించుకుంటుంది కానీ ఖరీదైనది, సులభం మరియు ప్రస్తుత యాక్సెస్ సిస్టమ్‌లకు అనుకూలంగా ఉండదు. ఫలితం ఇప్పటికే ఉన్న మరియు అభివృద్ధి చెందుతున్న భద్రతా వాతావరణాలను ఎదుర్కోగల బలమైన, బహుముఖ మరియు శక్తి-సమర్థవంతమైన పరిష్కారం.



చిత్రం 2: పద్ధతి

ISSN: 2583-9055 https://jcse.cloud/
CC BY

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

ప్రతిపాదిత స్మార్ట్ లాకింగ్ సిస్టమ్ కోసం ఫ్లో చార్ట్ పరికరాన్ని ప్రారంభించడంతో ప్రారంభమవుతుంది, తరువాత కీప్యాడ్, బయోమెట్రిక్ సెన్సార్ లేదా రెండింటి ద్వారా వినియోగదారు ఇన్‌పుట్ ఉంటుంది. సిస్టమ్ తగిన వాటి కోసం తనిఖీ చేస్తుంది ఆధారాలు లేదా కాదు; ఉంటే కాదు, ది వ్యవస్థ రెడీ అడగండి ది వినియోగదారు కు ఇన్పుట్ మళ్ళీ. తర్వాత సెన్సింగ్

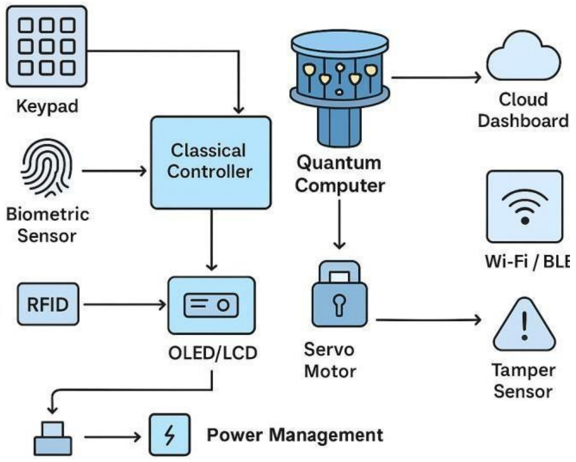
ఒక పాస్‌వర్డ్ లేదా బయోమెట్రిక్ నమూనా, ది ప్రామాణీకరణ ప్రక్రియ తనిఖీలు ది డేటా వ్యతిరేకంగా స్థానికంగా నిల్వ చేయబడింది లేదా క్లౌడ్ రికార్డులలో గుప్తీకరించబడింది. ప్రామాణీకరణ వైఫల్యం ఎర్రర్ నోటీసును మరియు సెట్ చేయబడితే, నిర్వాహకులకు హెచ్చరిక నోటీసును పంపుతుంది. విజయవంతమైన ప్రామాణీకరణ సర్వో మోటార్ తలుపు తెరిచేలా చేస్తుంది. కోసం ఒక ముందుగా నిర్ణయించిన సమయం ముందు స్వయంచాలకంగా లాకింగ్. వ్యవస్థ స్థితి ఉంది చూపబడింది ఆన్ ఒక ఆపరేషన్ సమయంలో LCD లేదా OLED డిస్ప్లే, మరియు అన్ని ఈవెంట్‌లు—విజయవంతమైన సమర్పణలు, విఫల ప్రయత్నాలు మరియు లాకౌట్ పరిస్థితులు - అవి నిల్వ చేయబడింది స్థానికంగా లేదా ప్రసారం చేయబడింది కు ఒక క్లౌడ్ ఆధారిత డాష్‌బోర్డ్ పర్యవేక్షణ కోసం. ఈ అధికారిక ప్రక్రియ సజావుగా పనిచేయడం, పారదర్శక వినియోగదారు అభిప్రాయం మరియు యాక్సెస్ అభ్యర్థనల సురక్షిత నిర్వహణను నిర్వహిస్తుంది.

4. ప్రయోగాత్మకమైనది సెటప్ మరియు అమలు

రూపొందించిన స్మార్ట్ లాకింగ్ సిస్టమ్ యొక్క ఆర్కిటెక్చర్ ఫిగర్ 3, హార్డ్‌వేర్, సాఫ్ట్‌వేర్ మరియు కమ్యూనికేషన్ లేయర్‌లను కలిపి, సురక్షితమైన ప్లాట్‌ఫామ్‌గా మిళితం చేస్తుంది. దీనికి దాని ప్రధాన భాగం ఉంది మైక్రోకంట్రోలర్, ఏది ఉంది ది ప్రాసెసింగ్ యూనిట్, లో ఛార్జ్ యొక్క ప్రామాణీకరణ, ఎన్క్రిప్షన్, మరియు మోటార్ నియంత్రణ. వినియోగదారు ఆధారాలు కీప్యాడ్, బయోమెట్రిక్ సెన్సార్ లేదా NFC/RFID రీడర్ ద్వారా సేకరించబడతాయి, అన్నీ వీటిలో GPIO పిన్‌లకు అనుసంధానించబడి ఉంటాయి. LCD లేదా OLED స్క్రీన్ జోడించబడుతుంది "పాస్‌వర్డ్ ఎంటర్ చేయండి," "యాక్సెస్ మంజూరు చేయబడింది," లేదా "యాక్సెస్ తిరస్కరించబడింది" వంటి తక్షణ అభిప్రాయాన్ని ప్రదర్శించండి. లాకింగ్ హార్డ్‌వేర్ మాడ్యూల్ దీని ద్వారా అమలు చేయబడుతుంది స్ట్రాప్ చేయబడిన సర్వో మోటార్ ఉపయోగించి ఆన్ ఒక నిర్దిష్ట అవుట్‌పుట్ పిన్ కు తిరగండి ది గొళ్ళెం మాత్రమే విజయం సాధించిన తర్వాత ధృవీకరణ. Wi-Fi లేదా బ్లూటూత్ MQTT లేదా HTTPS వంటి తేలికపాటి ప్రోటోకాల్‌లను ఉపయోగించి క్లౌడ్ సర్వర్‌లు మరియు మొబైల్ యాప్‌లతో కమ్యూనికేషన్ కోసం డిజైన్‌లో తక్కువ శక్తి మాడ్యూల్‌లను ఉపయోగిస్తారు. క్వాంటం-ప్రూఫ్ రోగనిరోధక శక్తితో అన్ని డేటా మార్పిడిని సురక్షితంగా ఉంచడానికి క్వాంటం-నిరోధక క్రిప్టోగ్రాఫిక్ లైబ్రరీలు ఫర్మ్‌వేర్‌లో ముందే ఇన్‌స్టాల్ చేయబడ్డాయి. నుండి దాడులు లో ది భవిష్యత్తు. ఈవెంట్ డేటా ఇష్టం లాగిన్ ప్రయత్నాలు, లాక్ రాష్ట్రం, మరియు శక్తి స్థాయిలు స్థానికంగా EEPROM లో నిల్వ చేయబడతాయి మరియు సురక్షితమైన క్లౌడ్ డాష్‌బోర్డ్‌తో సమకాలీకరించబడతాయి. విద్యుత్ నిర్వహణ ఉపవ్యవస్థ ఉంది సరఫరా చేయబడింది ద్వారా రీఛార్జబుల్ బ్యాటరీలు అనుబంధించబడిన ద్వారా సౌరశక్తి లేదా కైనటిక్ హార్వెస్టర్, పనిలేకుండా ఉన్నప్పుడు తక్కువ వినియోగాన్ని నిర్ధారించే స్లీప్

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

మోడ్‌లతో. హౌసింగ్‌లో ఇంటరప్ట్ పిన్‌లతో సంబంధంలో ట్యాంపర్ సెన్సార్‌లు కూడా ఉన్నాయి, ఇవి తక్షణమే అలారాలు లేదా నోటిఫికేషన్‌లను పంపుతాయి. ఎప్పుడు ప్రయత్నించారు బలవంతంగా ఎంట్రీ చేయబడింది. AI -ఆధారిత క్రమరాహిత్య గుర్తింపు పరికరంలో అమలు చేయగలదు. లేదా క్లౌడ్‌లో, పర్యవేక్షణ కోసం క్రూరమైన శక్తి లేదా అసాధారణమైన యాక్సెస్ ప్రయత్నాలు. ది ఆర్కిటెక్చర్ మాడ్యులర్, కాబట్టి డెవలపర్లు ఫేస్ రికగ్నిషన్ కెమెరాలు, హై-ఆర్డర్ వంటి తదుపరి తరం లక్షణాలను సులభంగా జోడిస్తారు బయోమెట్రిక్స్, లేదా క్వాంటం కీ పంపిణీ హార్డ్వేర్ లేకుండా పునఃరూపకల్పన అంతర్లీన తర్కం. ఫర్మ్‌వేర్ అనేది OTA పోస్ట్-క్వాంటమ్‌తో నవీకరించబడింది మరియు సంతకం చేయబడింది కోడ్-ఇంజెక్షన్ మాల్వేర్ రక్షణ కోసం అల్గోరిథంలు. ఇన్‌పుట్ నుండి ప్రాసెసింగ్, యాక్చుయేషన్, కమ్యూనికేషన్ వరకు స్టాక్ చేయబడిన ఆర్కిటెక్చర్, మరియు పర్యవేక్షణ, నిర్ధారిస్తుంది అది ప్రతి ఉపవ్యవస్థ గరిష్టీకరిస్తుంది భద్రత, సామర్థ్యం, మరియు స్కేలబిలిటీ. మొత్తంమీద, ఇది ఉంది ఒక ఘనమైన వేదిక కోసం పంపిణీ చేయడం వేగవంతమైన, వినియోగదారు-కేంద్రీకృతమైనది యాక్సెస్ మరియు IoT మరియు క్రిప్టోగ్రఫీలో తాజా ముప్పులను నివారించడం.



చిత్రం 3: వ్యవస్థ ఆర్కిటెక్చర్

CC BY

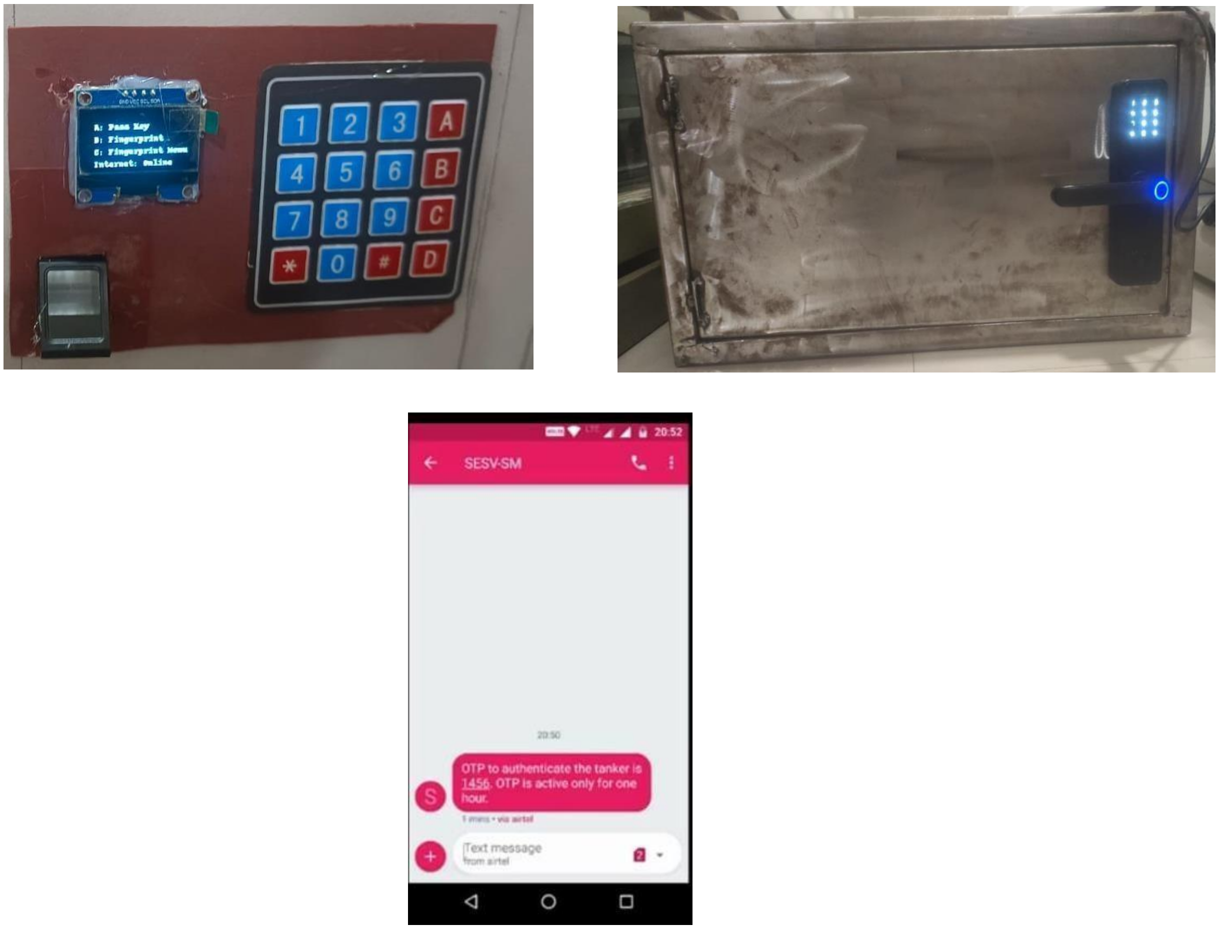
The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

5. ఫలితం విశ్లేషణ

ఈ ప్రోటోటైప్ వినియోగదారు ప్రామాణీకరణ మరియు యాక్సెస్ నియంత్రణలో స్థిరమైన పనితీరును ప్రదర్శించింది. IoT ఇంటిగ్రేషన్ ఈవెంట్ లాగింగ్ మరియు రియల్-టైమ్ హెచ్చరికను సులభతరం చేసింది. సిమ్యులేటెడ్ క్వాంటం-సేఫ్ ఎన్క్రిప్షన్ సాంప్రదాయ పాస్వర్డ్ పరిమాణాల కోసం సబ్-మిల్లీసెకన్ల లేటెన్సీ ఓవర్హెడ్ను ప్రదర్శించింది, ఇది ఎంబెడెడ్ లాక్లకు సాధ్యతను ధృవీకరించింది. సురక్షితమైన క్లౌడ్ ప్లాట్ఫామ్ను చేర్చడం వల్ల సిస్టమ్ యొక్క కార్యాచరణ మరియు తప్పు సహనం గణనీయంగా మెరుగుపడిందని పరీక్షలు నిర్ధారించాయి. తాళం చేస్తాను ఉండండి సామర్థ్యం గల యొక్క ఎగుమతి చేయడం యాక్సెస్ లాగ్లు (సమయం, వినియోగదారు ఐడి, విజయం/వైఫల్యం) నిజానికి నిర్వాహకులు కార్యాచరణను వీక్షించగలిగే సమయం వెబ్ డాష్బోర్డ్ లేదా మొబైల్ యాప్ ద్వారా. వైఫల్య హెచ్చరికలు, హెచ్చరికలను మార్చడం లేదా తక్కువ బ్యాటరీ క్లౌడ్ పుష్ నోటిఫికేషన్లు మరియు ఇమెయిల్ ద్వారా వెంటనే పంపబడ్డాయి. డాష్బోర్డ్ లాగిన్ ఫ్రీక్వెన్సీ, పీక్ వినియోగ సమయం మరియు AI ఇంజిన్ ద్వారా సృష్టించబడిన అనోమలీ ఫ్లాగ్లు వంటి విశ్లేషణలను అందించింది. క్లౌడ్-టు-లోకల్ కంట్రోలర్ సమకాలీకరణ నిర్వహించబడింది సరి లో ది ఈవెంట్ యొక్క నెట్వర్క్ వైఫల్యం గడువు ఒక తేలికైన కాషింగ్ వ్యవస్థ. ఫర్మ్వేర్ ఓవర్ ది ఎయిర్ (OTA) ను కూడా అప్గ్రేడ్ చేశారు, పోస్ట్-క్వాంటం తో సంతకం చేయబడింది కీలు అనధికారికంగా నిరోధించడానికి ట్యాంపరింగ్. జాప్యం కొలమానాలు ఉన్నాయి కింద 200లు ms కోసం లాగ్ అప్లోడ్ మరియు రిమోట్ అన్లాక్ అభ్యర్థనల కోసం 500ms కంటే తక్కువ, నిజ-సమయ ఆపరేషన్ వైపు సాక్ష్యమిస్తోంది. ఎన్క్రిప్షన్లో ఉపయోగించే క్వాంటం-సురక్షిత అల్గోరిథంలు ప్రసారం మరియు నిల్వ సమయంలో గోప్యంగా ఉంచబడ్డాయి. సాధారణంగా, వివిధ ప్రదేశాలలో స్మార్ట్ లాక్ని అమలు చేయడంలో కేంద్రీకృత పర్యవేక్షణ, అంచనా నిర్వహణ మరియు స్కేలబిలిటీలో క్లౌడ్ లేయర్ ముఖ్యమైనది.

CC BY

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025



చిత్రం 4: స్మార్ట్ తలుపు లాక్ వ్యవస్థ

6. ముగింపు

స్మార్ట్ లాక్ టెక్నాలజీస్ సాధారణ పాస్‌వర్డ్ ఆధారిత వ్యవస్థలకు మించి అభివృద్ధి చెందుతున్నాయి. ద్వారా సాంప్రదాయ మైక్రోకంట్రోలర్-ఆధారిత వ్యవస్థలతో IoT, AI మరియు క్వాంటం-నిరోధక క్రిప్టోగ్రఫీని అనుసంధానించడం ద్వారా, సంభావ్య ముప్పులను ఎదుర్కొనే సురక్షితమైన, అనుకూలీకరించదగిన వ్యవస్థలను మనం సృష్టించగలము. బ్యాటరీ-శక్తితో పనిచేసే విస్తరణల కోసం పవర్ ఆప్టిమైజేషన్ మరియు క్వాంటంను ఉపయోగించడం కీ సూపర్-సెక్యూర్ అప్లికేషన్ల పంపిణీ భవిష్యత్తులో కొన్ని దిశలు.

CC BY

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025

ప్రస్తావనలు

1. మకందర్, అజీజ్, ఆర్. బిరాదార్, మరియు ఎస్. తలవర్. "ఆర్డుయినో UNO ఉపయోగించి డిజిటల్ డోర్ లాక్ సెక్యూరిటీ సిస్టమ్." *ఇంటర్నేషనల్ రీసెర్చ్ జర్నల్ ఆఫ్ మోడరనైజేషన్ ఇన్ ఇంజనీరింగ్ టెక్నాలజీ అండ్ సైన్స్* 3.11 (2021). కదమ్, SG , "IoT -ఆధారిత స్మార్ట్ సెక్యూరిటీ సిస్టమ్," IJCSP, 2022.
2. ప్రీతి, సాదియా అక్తర్, జన్నతుల్ అఫ్రోస్, మరియు ఎండీ మహముదుల్ హసన్. "Rfid ఆధారిత స్మార్ట్ డోర్ లాక్ సెక్యూరిటీ వ్యవస్థ." *అమెరికన్ జర్నల్ యొక్క శాస్త్రాలు మరియు ఇంజనీరింగ్ పరిశోధన ఇ-ఐఎస్ఎస్ఎన్- 2348- 703ఎక్స్*
4.3 (2021).
3. పవిత్ర, బి., డి. నరేందర్ సింగ్, మరియు సుధీర్ కుమార్ శర్మ. "AI మరియు ML సాధనాలతో ప్రిడిక్టివ్ మరియు ఇంటరాక్టివ్ IOT డయాగ్నసిస్ సిస్టమ్." కంప్యూటేషనల్ ఇంటెలిజెన్స్ మరియు ఇన్ఫర్మేటిక్స్‌లో పురోగతి: ICACII 2019 యొక్క ప్రొసీడింగ్స్. స్ప్రింగర్ సింగపూర్, 2020.
4. ప్రజాపత్, సునీల్, మరియు ఇతరులు. "ఇంటర్నెట్ ఆఫ్ థింగ్స్ నెట్‌వర్క్‌ల కోసం క్వాంటం-సేఫ్ బ్లాక్‌చెయిన్-సహాయక డేటా ఎన్‌క్రిప్షన్ ప్రోటోకాల్." *క్లస్టర్ కంప్యూటింగ్* 28.1 (2025)
5. రోమన్, రాబర్టో, రోసారియో అర్జోనా మరియు ఇలుమినాడ బటురోన్. "ఒక క్వాంటం-సురక్షిత ప్రమాణీకరణ పథకం కోసం ఐఓటీ పరికరాలు ఉపయోగించి సమరూపమైన ఎన్క్రిప్షన్ మరియు బలహీనమైన భౌతిక మూసి వేయలేని సహాయక డేటా లేకుండా పనిచేస్తుంది." *ఇంటర్నెట్ ఆఫ్ థింగ్స్* 28 (2024): 101389.
6. సింగ్, డి. నరేంద్రర్, మరియు బి. పవిత్ర. "బహుళ అనువర్తనాల కోసం వెబ్ ఆధారిత రిమోట్ నావిగేషనల్ రోబోట్.
7. ఖాన్, మన్సూర్ అలీ, ముహమ్మద్ నవీద్ అమన్, మరియు బిప్లాబ్ సిక్దార్. "క్వాంటం గార్డ్: IoT పరికరాల కోసం క్వాంటం-ఆధారిత మాల్వేర్ రక్షణకు మార్గదర్శకత్వం." *2024 IEEE కాన్ఫరెన్స్ ఆన్ డిపెండబుల్ అండ్ సెక్యూర్ కంప్యూటింగ్ (DSC)*. IEEE, 2024
8. పవిత్ర, బి., సింగ్, డి. ఎన్., శర్మ, ఎస్. కె., & హష్మి, ఎం. ఎఫ్. (2023). చిత్తవైకల్యం అంచనా ఉపయోగించి నవల IOTM (ఇంటర్నెట్ ఆఫ్ థింగ్స్ ఇన్ మెడికల్) ఆర్కిటెక్చర్ ఫ్రేమ్‌వర్క్. ఇంటెలిజెంట్ డేటా అనాలిసిస్, 27(1_suppl), 29-45
9. యాదవ్, రేణు, మరియు అల్. "ఎ నవల ఆరోగ్య సంరక్షణ చట్రం కోసం పరిసర సహాయం చేయబడిన జీవించడం ఉపయోగించి ది ఇంటర్నెట్ వైద్యపరమైన విషయాలు (ఐఓఎంటీ) మరియు లోతైన నాడీ సంబంధిత నెట్‌వర్క్." కొలత: సెన్సార్లు 33 (2024): 101111.
10. రహాయు, అనిత. "IoT డోర్ లాక్ చేయడం ఒక సమీక్ష." 2024 ఇంటర్నేషనల్ కాన్ఫరెన్స్ ఆన్ ఇన్ఫర్మేషన్ మేనేజ్‌మెంట్ అండ్ టెక్నాలజీ (ICIMTech). IEEE, 2024.
11. జైనుద్దీన్, అహ్మద్ అన్వర్, మరియు అల్. "వినూత్నమైన ఐఓటీ స్మార్ట్ లాక్ వ్యవస్థ: మెరుగుపరుస్తోంది భద్రత ఫింగర్‌ప్రింట్ మరియు RFID టెక్నాలజీతో." మలేషియన్ జర్నల్ ఆఫ్ సైన్స్ అండ్ అడ్వాన్స్‌డ్ టెక్నాలజీ (2024): 360-365.

CC BY

12. రాజ్‌పుత్, సమ్మయ్య, మరియు అల్. "ఆధునికీకరణ హోమ్ పేజ్ రక్షణ: ఒక IoT -ఆధారితం విధానం తో స్మార్ట్ లాక్ మరియు ఆండ్రాయిడ్ అప్లికేషన్." 2024 ఐఈఈఈ 14వ అంతర్జాతీయ సమావేశం ఆన్ నియంత్రణ సిస్టమ్, కంప్యూటింగ్ మరియు ఇంజనీరింగ్ (ICCSCE). IEEE, 2024.

CC BY

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025
PP 260-269

Quantum-Resistant IoT Smart Locking Systems for Enhanced Security

B.Pavitra[1] , D.Narendar Singh[2], R.Nagaswetha[3]

[1,2,3]School of Computing, Dept of ECE, Anurag University, Hyderabad,Telangana-India

Corresponding Author *: pavitraece@anurag.edu.in

Abstract

Security has gained more significance in the globalized world of today. Mechanical locks are simple to override and provide minimal security against contemporary techniques of intrusion. The presence of IoT-based smart door locks offers reliable, easy-to-use solutions for residential, commercial, and industrial applications. This paper presents a better smart locking system employing Arduino UNO, embedded IoT devices, and emerging security paradigms like quantum- resistant cryptography and machine-learning-based authentication. With the implementation of quantum-resistant cryptographic algorithms and real-time cloud connectivity, the system proposed provides future-proof and scalable security.

Keywords:
Smart Locking System, Quantum Computing, IoT Security, Post-Quantum Cryptography, MQTT / Wi-Fi / BLE Communication

1.Introduction

Access control forms the foundation for physical and cyber security. Technologies have progressed from mechanical keys to electronic locks with RFID, OTP, and biometric verification. Door locks are now connected to mobile applications, home assistants, and cloud based devices that support remote monitoring and control as IoT devices continue to proliferate. These IoT devices are now more vulnerable to cyber attacks and hence require higher-level encryption and advanced anomaly detection. Quantum computing breakthroughs endanger conventional encryption techniques with quantum resistant cryptography (e.g., lattice-based cryptography) under research. Deployment of such algorithms in IoT-capable smart locks future-proofs security against forthcoming quantum- based threats. AI-based analytics further improve reliability through real-time detection of anomalous access patterns and brute-force attempts. This paper

CC BY

suggests an Arduino UNO and IoT

hardware-implemented reinforced door lock with the optional feature of using quantum-safe encryption and monitoring over the cloud.

2. Literature Survey

[1] Akshaya Krishnadas Bhat et al. The emergence of smart door lock technology is a precursor to the rapid integration of electronics, IoT, and cybersecurity. Initial researches, for example, by Bhat et al., developed password-protected doors based on Arduino boards, showing that low-cost microcontrollers could offer enhanced home security than standard mechanical locks. [2] Prabhakar et al. took it a step further by suggesting Arduino UNO-based locks that were economical and simple to install in offices, homes, and schools. Kumar et al. suggested Bluetooth- based locks where Bluetooth served as the communication bridge between smartphones and Arduino, showcasing the capability of mobile-access control. Further developments have shown longer-distance connectivity through Wi-Fi modules to synchronize door locks with cloud dashboards to log events and verify status. RFID verification is a widespread contactless alternative, and fingerprint and facial recognition sensors offer improved, multi-factor security. [3] Low-power IoT protocols like MQTT and the Matter standard enable more optimal communications and device interoperability and position smart locks at the hub of bigger smart- home systems. Energy efficiency is also in focus, e.g., for battery-powered locks, resulting in low- power hardware and harvesting energy from sunlight or kinetic sources. Simultaneously, AI-based analytics were used to detect brute-force attacks or abnormal patterns of logins, raising the resistance against illegal access. Recent efforts focus on the impending quantum computer threat that would be capable of breaking classical encryption methods. [4] Post-quantum cryptography as lattice-based encryption and hash-based signatures was demonstrated to support embedded hardware with little latency, and NIST's standards guide in 2024 control the selection of quantum- resistant schemes. There are also articles investigating the application of quantum key distribution in ultra-high-security environments. Hybrid systems incorporating PINs, biometrics, RFID, and anomaly detection demonstrate a multi-layered defense position, and intrusion sensors and tamper- proof encasements offer additional physical strength. Edge computing is suggested for reducing authentication latency through local credential processing, and sustainable design is aimed at long battery life and energy harvesting. Usability testing examines end-user adoption of biometric and quantum-secure locks and finds that familiarity and feedback enhance adoption. As a whole, this collection of research traces development from basic keypad locks to advanced, encrypted devices mashups of IoT, AI, and quantum-resistant crypto. This work expands upon these findings by integrating Arduino, IoT networking, anomaly detection, and post-quantum encryption to create a future-proof, scalable

CC BY

security solution.

3. Methodology

Design strategy for an intelligent locking system of the next generation is centered around the integration of an Arduino UNO controller with IoT, quantum-resistant cryptography, and accessible access mechanisms. Start by defining the Arduino UNO as the master processing unit that would control all the subsystems, such as authentication, motor drive, and communication of data. A user types in a password or biometric information using an input interface, such as a plain 4×4 keypad, capacitive touch screen, or advanced biometric sensors like fingerprint or facial recognition readers. Such inputs are checked locally by the Arduino against stored credentials or authenticated remotely through a secure cloud server via Wi-Fi or Bluetooth Low Energy (BLE). To avoid credential stealing or eavesdropping, communication between the device and cloud services is Transport Layer Security (TLS) encrypted or, where necessary, quantum-resistant algorithms like lattice-based or hash-based encryption libraries. After successful authentication, the Arduino sends the control signals to a servo motor operating the lock mechanism to rotate the latch to unlock for an interval duration. On failure of authentication, the system is locked, and feedback in real time from an LCD or OLED display informs the user of "WRONG PASSWORD" or "ACCESS DENIED." In case of repeated failures, an alarm is received by the administrator smartphone or cloud dashboard, and the system can be set to enter lockout mode to prevent brute- force attacks. For supporting IoT functionality, the system figure 1, has a Wi-Fi module (e.g., ESP8266/ESP32) or BLE hardware that supports event logging, remote unlocking, and firmware updates. The information is communicated using light-weight protocols like MQTT or HTTPS, such that support for smart-home hubs based on the Matter standard is guaranteed. AI-driven anomaly detection algorithms can be executed locally or in the cloud, monitoring patterns of access and marking suspicious activity in real time. Power management is taken care of by the use of low-consumption hardware, sleep modes, and alternative renewable power in the form of small solar panels or kinetic charging. The servo motor is also PID-tuned to run smoothly and stably and reduce power consumption. Everything from the Arduino to the motor, keypad, and display is inside a tamper-evident case with intrusion detectors that sound alarms when the casing is opened. System maintains a software architecture that supports modular upgrades so that new authentication methods like RFID cards, NFC mobile phones, or even quantum key distribution for ultra-secure centers can be added by developers. Access logs and performance metrics are kept on local storage and synced to cloud storage for reliability even during network outages. It has a multi-layered security strategy, with local authentication augmented with encrypted cloud-

CC BY

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025
PP 260-269

based verification and regular firmware updates signed with post-quantum cryptographic keys to protect against unauthorized code injection.

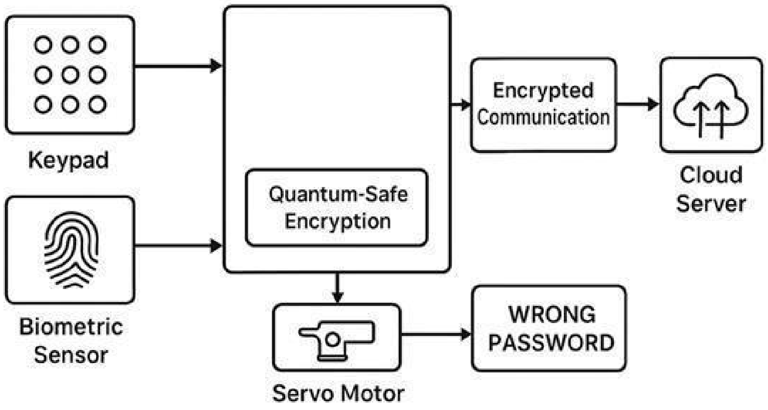


Figure 1: Quantum-Resistant based IoT Smart Locking Systems

Prototype testing also covers assessment of authentication rate, encryption penalty, servo response time, and power consumption under typical domestic and office environment usage conditions. Stress tests include emulation of repeated unsuccessful login attempts and testing the lockout and alert features. By this approach, the suggested smart lock capitalizes on IoT, AI, and quantum-resistant cryptography but is not pricey, easy, and compatible with current access systems. The outcome is a strong, versatile, and power-efficient solution that can face existing and emerging security environments.

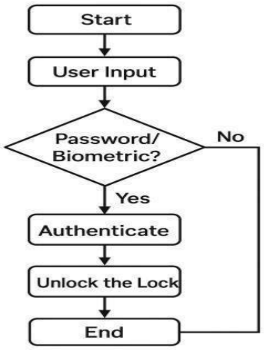


Figure 2: Methodology

The flow chart for the smart locking system proposed starts with the device initialization, followed by user input via a keypad, biometric sensor, or both. The system checks for appropriate credentials or not; if not, the system will ask the user to input again. Upon sensing

CC BY

a password or biometric sample, the authentication process checks the data against stored locally or encrypted in the cloud records. Authentication failure sends an error notice and, if set, an alert notice to administrators. Successful authentication has the servo motor open the door for a predetermined time before automatically locking. System status is shown on an LCD or OLED display during operation, and all events—successful submissions, failed attempts, and lockout situations—are stored locally or relayed to a cloud-based dashboard for monitoring. This formalized process maintains smooth operation, transparent user feedback, and secure management of access requests.

4. Experimental Setup and Implementation

The architecture figure 3, of the designed smart locking system is such that it combines hardware, software, and communications layers into a combined, secure platform. It has its core microcontroller, which is the processing unit, in charge of authentication, encryption, and motor control. The user credentials are gathered through a keypad, biometric sensor, or NFC/RFID reader, all of which are connected to the GPIO pins. An LCD or OLED screen is added to display instant feedback like "Enter Password," "Access Granted," or "Access Denied." The locking hardware module is implemented by using a servo motor strapped on a specific output pin to turn the latch only after successful verification. Wi-Fi or Bluetooth Low Energy modules are utilized in the design for communication with cloud servers and mobile apps using light- weight protocols like MQTT or HTTPS. Quantum-resistant cryptographic libraries are pre- installed in the firmware to secure all data exchange with quantum-proof immunity from attacks in the future. Event data like login attempts, lock state, and power levels are locally stored in EEPROM and synchronized with a secure cloud dashboard. A power management subsystem is supplied by rechargeable batteries complemented by solar or kinetic harvester, with sleep modes ensuring low consumption during idle times. The housing also features tamper sensors in contact with interrupt pins, which instantaneously send alarms or notifications when attempted forced entry is made. AI-driven anomaly detection can run on- device or in the cloud, monitoring for brute-force or aberrant access attempts. The architecture is modular, so developers easily add next-generation features like face recognition cameras, higher-order biometrics, or quantum key distribution hardware without redesigning underlying logic. Firmware is OTA updated and signed with post-quantum algorithms for code-injection malware protection. The stacked architecture, from input to processing, actuation, communication, and monitoring, ensures that every subsystem maximizes security, efficiency, and scalability. Overall, this is a solid platform for delivering speedy, user-focused access and fending off the latest threats in IoT and cryptography.

CC BY

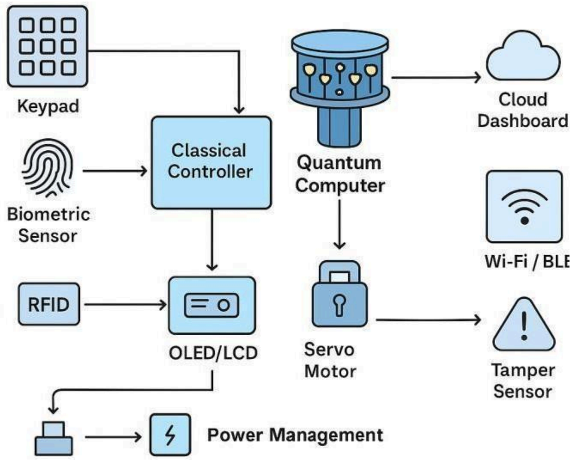


Figure 3: System Architecture

5. Result Analysis

The prototype demonstrated sustained performance in user authentication and access control. IoT integration facilitated event logging and real-time alerting. Simulated quantum-safe encryption demonstrated sub-millisecond latency overhead for conventional password sizes, which attested to feasibility for embedded locks. Tests confirmed that inclusion of a secure cloud platform substantially improved the functionality and fault tolerance of the system. The lock would be capable of exporting access logs (time, user ID, success/failure) in real time where administrators would be able to view activity through a web dashboard or mobile app. Failure attempt warnings, tamper alerts, or low battery were sent immediately through cloud push notifications and email. The dashboard offered analytics such as login frequency, peak usage time, and anomaly flags created by an AI engine. Cloud-to-local controller synchronization was maintained even in the event of network failure due to a light- weight caching system. Firmware was also upgraded over the air (OTA), signed with post- quantum keys to prevent unauthorized tampering. Latency metrics were under 200 ms for log upload and under 500 ms for remote unlock requests, testifying towards real-time operation. Quantum-secure algorithms used in encryption were kept confidential during transmission and storage. In general, the cloud layer was important in centralized monitoring, predictive maintenance, and scalability in deployment of the smart lock in various locations.

CC BY

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 3, No 11, Nov 2025
PP 260-269

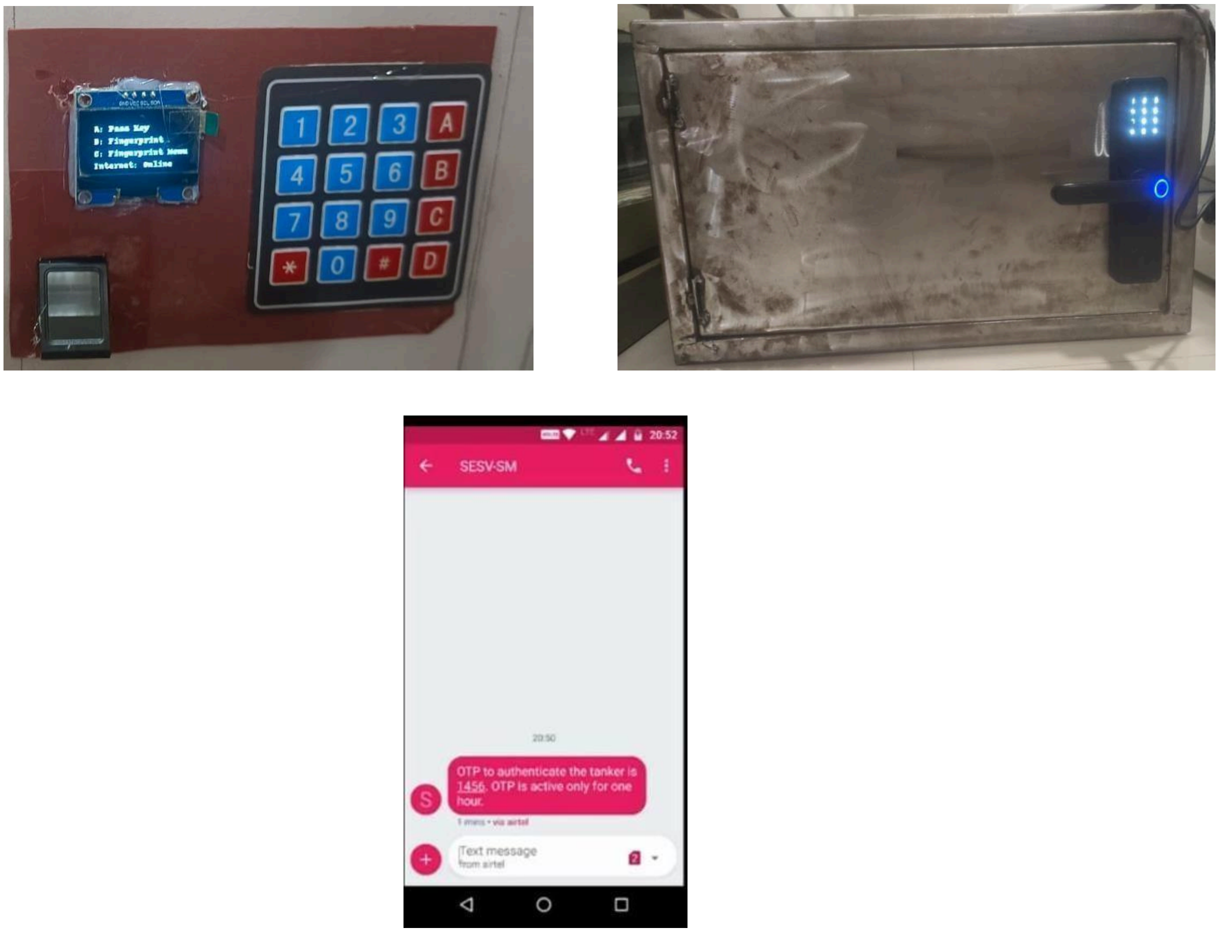


Figure 4: Smart Door lock system

6. Conclusion

Smart lock technologies are evolving beyond simple password-based systems. By integrating IoT, AI, and quantum-resistant cryptography with traditional microcontroller-based systems, we can create secure, adaptable systems that stay in front of potential threats. Power optimization for battery-powered deployments and using quantum key distribution for super-secure applications are some of the directions in the future.

CC BY

References

1. Makandar, Aziz, R. Biradar, and S. Talawar. "Digital Door Lock Security System using Arduino UNO." *International Research Journal of Modernization in Engineering Technology and Science* 3.11 (2021). Kadam, S.G., "IoT-Based Smart Security System," IJCSP, 2022.
2. Prity, Sadia Akter, Jannatul Afrose, and Md Mahmudul Hasan. "Rfid based smart door lock security system." *American Journal of Sciences and Engineering Research E-ISSN- 2348-703X* 4.3 (2021).
3. Pavitra, B., D. Narendar Singh, and Sudhir Kumar Sharma. "Predictive and Interactive IOT Diagnosis System with AI and ML Tools." Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2019. Springer Singapore, 2020.
4. Prajapat, Sunil, et al. "Quantum-safe blockchain-assisted data encryption protocol for internet of things networks." *Cluster Computing* 28.1 (2025)
5. Román, Roberto, Rosario Arjona, and Iluminada Baturone. "A quantum-safe authentication scheme for IoT devices using homomorphic encryption and weak physical unclonable functions with no helper data." *Internet of Things* 28 (2024): 101389.
6. Singh, D. Narendhar, and B. Pavitra. "Web based Remote Navigational Robot for Multiple Applications.
7. Khan, Mansoor Ali, Muhammad Naveed Aman, and Biplab Sikdar. "Quantum Guard: Pioneering Quantum-Based Malware Defense for IoT Devices." *2024 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 2024
8. Pavitra, B., Singh, D. N., Sharma, S. K., & Hashmi, M. F. (2023). Dementia prediction using novel IOTM (Internet of Things in Medical) architecture framework. Intelligent Data Analysis, 27(1_suppl), 29-45
9. Yadav, Renu, et al. "A novel healthcare framework for ambient assisted living using the internet of medical things (IOMT) and deep neural network." Measurement: Sensors 33 (2024): 101111.
10. Rahayu, Anita. "IoT Door Locking a Review." 2024 International Conference on Information Management and Technology (ICIMTech). IEEE, 2024.
11. Zainuddin, Ahmad Anwar, et al. "Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology." Malaysian Journal of Science and Advanced Technology (2024): 360-365.
12. Rajput, Summaiya, et al. "Modernizing Home Protection: An IoT-Driven Approach with Smart Lock and Android Application." 2024 IEEE 14th International Conference on Control System, Computing and Engineering (ICCSCE). IEEE, 2024.

CC BY