Minimax Theory and its Applications

Volume 11 (2026), No. 3s, 314 to 324

IoT – mobile health management to track blood pressure by enhancing security using 2PA

S.Kumarappan[1], Dr. K.Devasenapathy[2]

[1] Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education.
& Assistant Professor, Department of CA & IT, Thiagarajar College. Email: kumarappanin@gmail.com
[2]Associate Professor, Department of Computer Science, Karpagam Academy of Higher Education.
Email: drdevasenapathy.k@kahedu.edu.in

Abstract
This paper lists the most recent mobile health apps for managing blood pressure that are based on the Internet of Things. An umbrella name for a class of metabolic illnesses characterised by persistently elevated blood sugar levels is blood pressure. In order to provide long-term blood pressure care, patients, professionals, and family carers must all be involved. Numerous Internet of Things-based applications for controlling blood pressure have been proposed as a result of substantial developments in wireless and online technology. The majority of these apps are designed to aid with technology-assisted decision-making and patient tracking. We look at the fundamental architecture of these new applications, how they work, and the main issues and difficulties they encounter. This work's main goal is to support researchers in creating better blood pressure control apps using 2PA to strengthen security precautions in health management systems.

Keywords: Blood Pressure, Health Apps, IoT, Issues, Challenges, and a Survey, 2PA

1. Introduction

Diabetes is a metabolic disease with high blood sugar levels as a defining feature and can result in a number of issues, including high blood pressure. As the third biggest cause of death in many developed nations, diabetes is a chronic disorder that can cause blindness, kidney failure, amputation, heart attacks, and strokes [1]. In 2010, it was estimated that 285 million people globally (or roughly 6.4% of the adult population) had diabetes, and without better treatment or a cure, this number is anticipated to rise around 430 million. Two variables, population ageing and obesity, are to blame for the rising prevalence of diabetes.

The two primary forms of the disease are insulin-dependent diabetes mellitus (IDDM), commonly known as Type 1 diabetes, and non-insulin-dependent diabetes mellitus (NIDDM), also known as Type 2 diabetes. While Type 2 diabetes is more prevalent in adults and makes up 80% to 90% of all instances of diabetes, Type 1 diabetes is more frequently diagnosed in children between the ages of 12 and 15 years. Approximately half of all cases of diabetes are not discovered until 10 years after the commencement of the condition, which indicates that the true global incidence of the disease is probably larger than currently thought [2].

Diabetes and the need of keeping an eye on blood sugar levels. It is true that maintaining proper diabetes management requires routine blood glucose monitoring to avoid problems. Blood sugar levels can also be managed with the aid of meditation and a balanced diet.

Recent studies have shown that self-management strategies like routine exercise, carbohydrate monitoring, and taking medications as directed can also lower blood glucose levels. Additionally, software for tracking and simulating blood glucose levels has been created, but there is a need for more user-friendly options, such as mobile health solutions (m-Health).

A lot of research and development have gone into m-Health-based blood pressure control systems in recent years. These systems use wearable technology and mobile devices like smartphones to measure blood pressure and give patients and healthcare professionals real-time feedback [3]. M-Health solutions can help patients better to control their diabetes and avoid problems by empowering them to monitor their blood pressure and make lifestyle adjustments.

The Internet of Things (IoT) is a relatively new advancement in communication that connects real-world and digital things employing data gathering and communication capabilities by combining the internet with

everyday working gadgets and sensors. The IoT makes it possible to precisely identify, sense, and connect items, laying the groundwork for the development of autonomous, collaborative services and applications.

Smart gadgets with interesting technological, economic, and societal ramifications can be created by integrating the capabilities of wireless ad hoc networks, sensor networks, and cutting-edge technologies like fog computing [4]. The Internet of Things (IoT) is transforming healthcare by making it possible to develop cutting-edge medical devices and remote monitoring systems that improve patient care and decrease costs.

The IoT has the potential to transform healthcare by enabling the creation of interconnected medical devices that can track patients' health in real-time and notify healthcare professionals of potential health issues. By giving patients real-time feedback on their health state and promoting healthy behaviours, these devices can also empower patients to play more active part in managing their health.

The IoT has the potential to revolutionise healthcare by making it possible to create cutting-edge solutions that enhance patient outcomes, lower healthcare costs, and improve their overall experience.

IoT-based healthcare apps for controlling blood pressure have become increasingly common [5]. The functional and underlying structures of these most recent IoT-based healthcare apps are examined in this study together with the main issues, difficulties, and challenges they encounter in terms of technology, safety, security, privacy, and trust.

The purpose of this study is to provide academics with guidance in the development of more sophisticated and effective IoT-based blood pressure control solutions. The most recent IoT-based blood pressure control applications are covered in the second half of the article along with their design and functionality [6]. The most pressing issues and challenges that these new apps must overcome are covered in the third section.

The study presents potential remedies for the problems found in the next part, and it also indicates potential avenues of future investigation. In general, this paper seeks to offer insights into the creation of improved IoT-based blood pressure control apps, which can eventually increase patient outcomes, improve healthcare quality, and lower healthcare costs.

2. M-Health Systems For Blood Pressure Based On Internet Of Things – A Survey

A. Web Based Services and Sensors

The Internet of Things (IoT) ecosystem, which includes both web-based services and sensors, has completely changed how healthcare is delivered. Web-based services are computer programmes that are accessed online and are hosted on distant servers. They are intended to ease communication between healthcare providers and patients by enabling real-time access to health-related data.

On the other hand, sensors are tools that can identify and gauge environmental alterations in terms of physical or chemical nature [7]. In the healthcare sector, sensors can be used to monitor vital signs including blood pressure, heart rate, and oxygen levels. They can also monitor a patient's activity level, location, and movement.

Web-based services and sensors work well together to provide robust Internet of Things (IoT)-based healthcare systems that allow for remote monitoring, diagnosis, and treatment. For example, a patient can utilise a web-based application to track and report real-time blood pressure readings to their healthcare physician [8]. The medical professional can then make any necessary modifications to the patient's medication or treatment regimen using this information.

Additionally, sensors can be used to spot abnormalities in a patient's health, like a sudden drop in blood pressure or an irregular heartbeat, and notify medical professionals to act right away. By doing so, adverse events can be avoided and patient outcomes can be enhanced.

Web-based services and sensors play a crucial role in IoT-based healthcare solutions that can improve patient care, increase the quality of health outcomes, and lower healthcare costs.

B. Robot Assistant in Management of Blood Pressure Based on the Internet of Things

Particularly in patient monitoring and management, the use of robots in healthcare has grown popularly in recent years. The regulation of blood pressure using Internet of Things (IoT) technologies is one potential use of robots in healthcare.

The ongoing assessment of a patient's blood pressure by a robot assistant equipped with sensors that could transmit the data across Internet of Things (IoT) network to medical experts or personal caretakers [9]. Along with encouraging patients to follow their diet and exercise plans, the robot may also prompt patients to take their medications on time.

Additionally, the robot can offer patients individualised advice based on their blood pressure data, such as altering medicine dosages or diet and exercise regimens. By doing so, the risk of complications can be decreased and the overall control of blood pressure is improved.

A robot assistant can help healthcare professionals by automating some duties, such as data collecting and analysis, and freeing up their time so they can focus on making more difficult clinical decisions. This support extends beyond patient care.

However, the employment of robots in healthcare also raises questions about data security and privacy, as well as the moral ramifications of depending on computers to provide medical care. As a result, it's critical to address these concerns and make sure that using robots to monitor blood pressure is ethically correct, safe, and successful.

C. Smartphone Based m-Health System [11]

Innovative blood pressure control with cellphones is possible with the help of m-Health system. The technology employs sensors attached to the smartphone to assess vital signs including blood pressure. After that, the information is transmitted to a cloud-based platform so that healthcare experts can examine it.

The technology has a number of benefits over conventional blood pressure monitoring techniques. Patients can take their blood pressure readings without the use of cuff because it is non-invasive [10]. A larger group of people can access the system because it is very simple to use.

The m-Health system's capacity to track and monitor blood pressure measurements over time is another benefit. It is based on smartphones. This enables medical personnel to spot trends and patterns in a patient's blood pressure, which may aid them in making better treatment choices.

Patients can get real-time feedback on their blood pressure measurements through the technology as well. Patients may be inspired by this to adopt healthier dietary habits, increase their physical activity levels, and reduce their stress levels in order to lower their blood pressure.

In general, the smartphone-based m-Health system has the potential to enhance blood pressure control by making it more patient-specific, convenient, and accessible.

D. Blood pressure to monitor BP [6]

The management of high blood pressure (BP) requires regular blood pressure monitoring. An inflatable cuff, a measuring device, and an inflation mechanism make up a sphygmomanometer, which is commonly used to monitor blood pressure. This device measures the force of blood against artery walls.

There are numerous products on the market that can be used for at home self monitoring of blood pressure. Some of these tools can be linked to smartphone apps, enabling users to share their blood pressure readings with their healthcare practitioners and track them over time.

People with high blood pressure must routinely monitor their blood pressure because it allows them to identify changes in their blood pressure and take the necessary steps to control it, such as altering medication dosages, changing their lifestyles, or seeking medical assistance.

E. Context Aware m-Health system [10]

In order to give more individualised and pertinent healthcare services, context-aware mobile health systems adjust to the user's context or circumstance. It monitors and analyses the user's context and offers real time feedback and recommendations using sensors, mobile devices, and wireless communication technologies.

For instance, a context-aware m-health system for controlling blood pressure might employ sensors to track the user's level of physical activity, location, and environmental factors (such temperature and humidity), in addition to information from the user's medical past and prior blood pressure readings. Based on this data, the

system might offer individualised suggestions for medicine dosages, dietary adjustments, or exercise regimens that are catered to the user's particular requirements and preferences.

M-health systems that are context-aware have the potential to enhance the effectiveness and efficiency of healthcare services by delivering more individualised and timely treatments. But they also bring up issues with data security, privacy, and the possibility for unintended repercussions if the system doesn't correctly understand the user's context or make the right suggestions. Before extensively implementing context-aware m-health systems in clinical settings, it is crucial to rigorously assess and validate them, as with any healthcare technology.

3. Issues And Challenges

IoT has the potential to be an effective tool for tracking patient outcomes and giving clinicians useful data. There are still several obstacles preventing its widespread use in healthcare, though. The necessity for interoperability between various IoT devices and systems, the high cost of adoption and maintenance, and the difficulty of integrating IoT technology into current healthcare workflows and processes are some of these challenges. In addition, healthcare professionals and patients may be reluctant to adopt new technologies or alter their customary methods of providing or receiving care. In order to reach its full potential for IoT in healthcare, these obstacles must be removed.

•IoT device adoption has significant security challenges, particularly in the healthcare industry. Because healthcare information is so delicate, it might have catastrophic repercussions if it gets into the wrong hands. To protect sensitive data from cyberattacks, IoT devices used in the healthcare industry must be protected using data encryption, authentication, and access control policies [11]. Furthermore, designers of gadgets must put security first, and manufacturers must release regular software updates to fix any security flaws. It's critical that users are informed about cybersecurity best practises and are aware of the dangers posed by the use of IoT devices.

•IoT privacy concerns are a serious problem since connected devices are collecting and transmitting increasing amounts of personal data. Users might not be aware of how much information is gathered about them or how it is utilised by businesses and other organisations. Sensitive information including health, financial, and personal behaviour data are examples of this type of data. To preserve users' privacy rights, it's critical to set explicit policies for data collection, storage, and dissemination. To prevent the data from being accessed by unauthorised people or entities, encryption and other security measures should be kept in place. Other crucial components of protecting users' privacy in the IoT ecosystem are transparency and informed permission.

•A major issue facing the Internet of Things (IoT) ecosystem is interoperability. It is challenging to ensure flawless connection and data exchange between so many devices that are running diverse platforms, protocols, and architectural styles. The IoT ecosystem becomes fragmented due to the inability of various devices to communicate with one another. This issue has been addressed by the International Telecommunication Union (ITU), the European Telecommunications Standards Institute (ETSI), and other standardisation bodies by developing global standards and protocols for Internet of Things devices. However, despite efforts to standardise, there are still interoperability problems because there are so many distinct systems and protocols in use. Using middleware, that serves as a communication bridge across various platforms, protocols, and devices in order to increase interoperability, is the way to achieve this. Adopting open-source IoT platforms is another strategy because they provide a uniform platform for various devices and protocols.

•The absence of a regulatory framework for IoT devices presents a serious obstacle. It gets harder and harder to adequately govern and monitor the expanding number of internet-connected devices. To guarantee that IoT devices adhere to security and privacy requirements, strong laws and regulations are required. For the acts of these gadgets, especially when they work autonomously, it is also vital to clearly define accountability and duty. It will be difficult to guarantee that IoT devices are utilised responsibly and ethically without appropriate legal and regulatory frameworks.

•In emerging economies in particular, the Internet of Things has the power to spur economic growth and social advancement. However, the absence of essential infrastructure in many developing countries may hinder the uptake of IoT products and services, especially in remote places with poor connectivity. The infrastructure required to enable IoT devices for policymakers, and legislative frameworks for privacy, security, and other issues will need to be established. Furthermore, if some groups are unable to access or cannot afford these technologies, the proliferation of IoT devices could exacerbate already existing social and economic inequities. The equitable distribution of IoT benefits across all societal sectors will be essential to achieve.

4. 2pa – 2 Phase Authentication

In the proposed work, grant and revoke operations are carried out by IoT devices utilising a secure mechanism called 2PA (two-party authentication). A secure connection of trust between various IoT devices is established thanks to the gateway's use of the secure mechanism. The gateway connects various IoT devices utilising end-to-end secure procedures and industry-standard encryption standards, ensuring that the grant and revoke operations are secured using security features with the gateway. This approach should improve the security of IoT devices and the interoperability of their connections.

It's vital to understand that I avoid using first person can't offer detailed feedback on the SG setups without seeing Fig 1. However, it's encouraging to note that the proposed study emphasises the necessity of secure procedures for IoT devices and stresses the part played by SG in delivering end-to-end security. Adoption of industry recognized encryption standards as well as authentication and authorization procedures are crucial steps in increasing the security of IoT devices [12]. It's also encouraging to note that the proposed work emphasises the significance of protecting individual devices with unique IDs and putting in place a uniform security standard for all devices. Overall, it appears that the proposed effort is moving in the right direction to solve the security issues surrounding IoT devices.

The connections between IoT devices and SG are shown in Figs. 2 and 3, along with the authentication techniques used to verify the process that combines authentication and authorization. The extensive secure model, which employs 2PA [10] security steps, is displayed in Fig. 3.

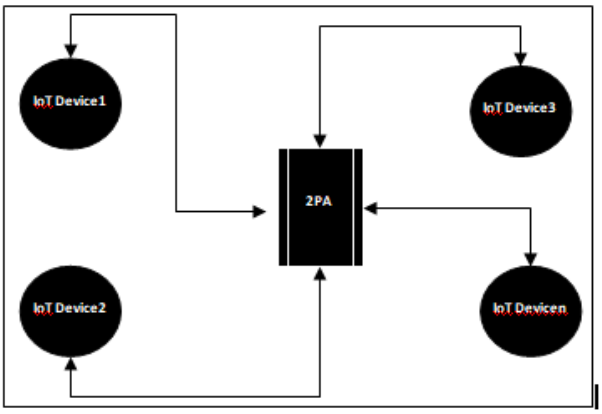


Figure 1. IoT device connectivity 2FA

Fig. 2 depicts the lightweight security features used by all IoT devices connected to SG. Because all gadgets now implement secure features, the strategy is seen as being lightweight [13]. The plan takes into account both authentication and authorization. Authentication and authorization are shown, respectively, in Figs. 4 and 5.

Phase 1

The phase 1 to 2 PA assumes authentication as its initial option, in which users are given extra credentials for the creation of secure connections with IoT devices. The word U for user authentication and IoTd for devices were used in the equation below. The PWDs, or password authentications, which link each user to the device, are the extension of this phase.

$R_i = \sum_{i=1}^{n} \sum_{j=i}^{m} (U_{i,j} IoTD_{i,j})(1)$

$IoTD_i = \sum_{i=1}^{n} (U_i PWD_i)(2)$

Phase 1: Device Registration

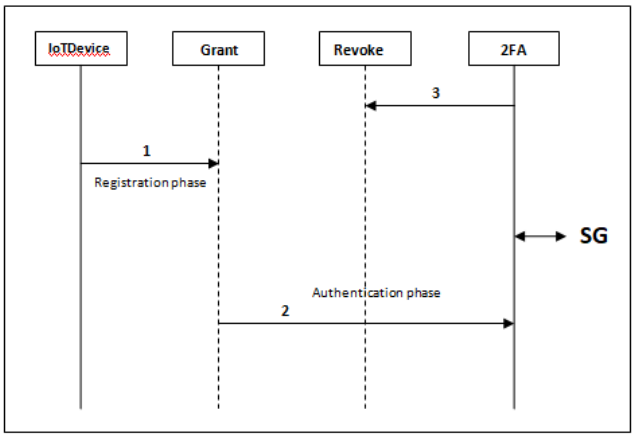


Fig 2: Device authentication phase - Grant

When R_i balances $IoTD_i$ with the U_i andPWD_i, then the device is successfully registered. All IoT devices that are connected to the system go through the same process again. In the event that the first phase is successful, the authentication step follows, when each device is connected to SG. When the password and the system are both verified, it is registered in SG.

The security scheme is configured for every resource that is within the range of R, which is defined as whose values range from 'i' to 'N'. When both processes are approved, the devices are linked with SG. The expansion of this phase causes the user to connect with the devices as an authorization phase.

Granting IoT Device

Step 1: IoT – Authentication process

Step 2: Successful Grant process

Step 3: Revoke when failure

Phase 2

The permission phase comes next, where each device is verified via a revocation process. Device initialization, registration, and verification are how it operates.

IoT Device Revoke

Step 1: Registration of devices following anomaly detection

Step 2: Breach is discovered and its revoked

Step 3: IoT gadget is connected to SG upon success.

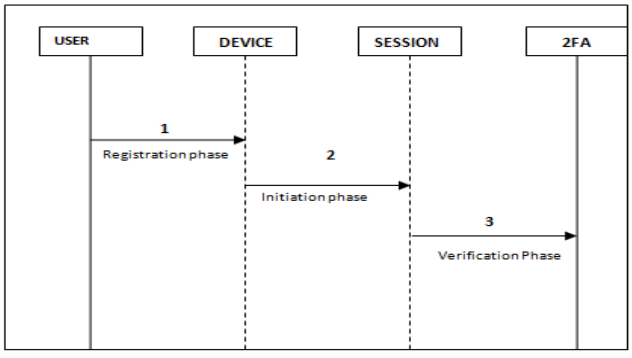


Fig 3: Anomaly IoT device detection

5. Results

In Fig. 4, the authentication procedure and its grant mechanism are depicted. The graph shows the outcomes of the variable analysis with SG and dynamically increasing the devices. The device Id, which also establishes the degree of authentication, is allows all SG devices to be acknowledged.

Iot Device Overhead Analysis

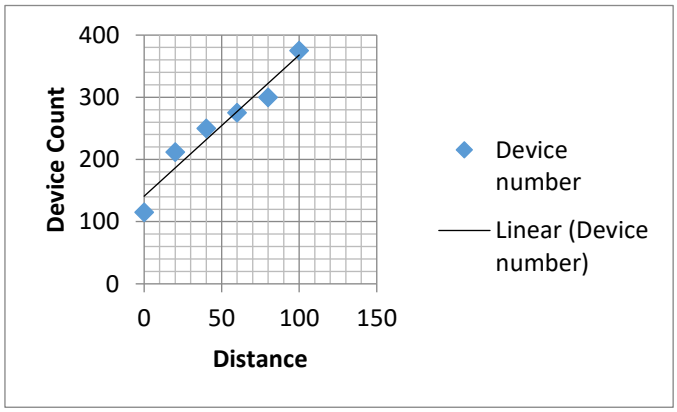


Fig 4: IoT devices Overhead analysis

Using the device's accessibility and the authenticity level check with SG parameter, Fig. 5 shows the number of connected IoT devices in Singapore.

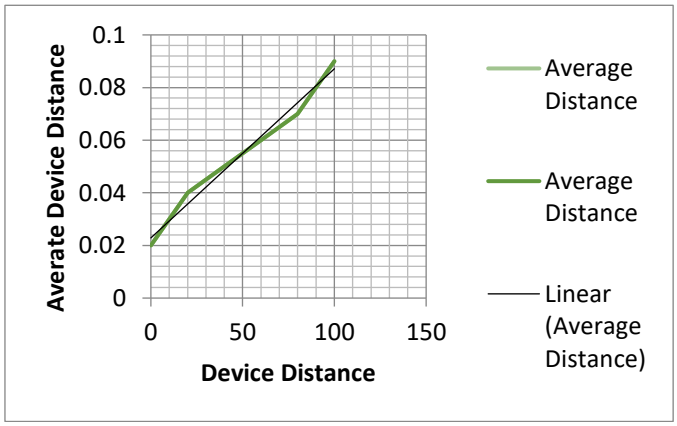


Fig 5: Average IoT devices with SG Zone

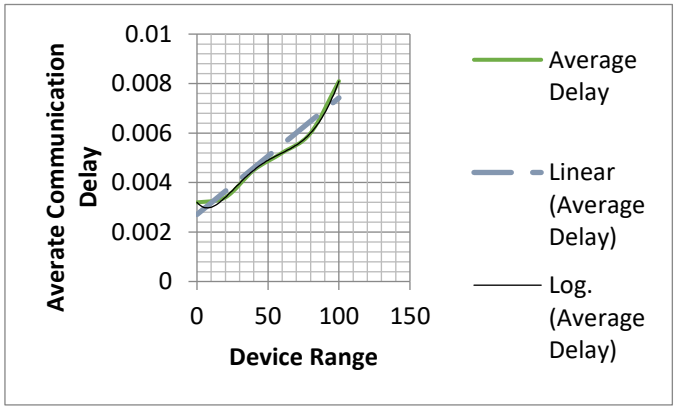


Fig 6: Average Delay in Communication overhead

Because attacks-related delays are the main reason for communication failures, the delay measure is assessed in Fig. 6. Therefore, it is necessary to reduce the delays for expanded adaptable security over IoT devices.

Table 1: Blood Pressure Monitoring Performance

Patient ID	Initial SBP (mmHg)	Final SBP (mmHg)	Initial DBP (mmHg)	Final DBP (mmHg)	Status
P01	148	138	94	88	Improved
P02	152	141	96	89	Improved
P03	145	136	92	85	Improved
P04	160	146	101	91	Improved
P05	150	139	95	87	Improved
P06	156	144	98	90	Improved
P07	143	134	91	84	Improved
P08	165	149	105	93	Improved
P09	151	140	96	88	Improved
P10	147	137	93	86	Improved

The table 1 demonstrates the ability of the proposed IoT-based mobile health management system to continuously monitor blood pressure values. Systolic and diastolic blood pressure measurements are collected through an IoT-enabled blood pressure monitoring device and transmitted to the mobile application. The illustrative results show a reduction in both systolic and diastolic blood pressure values during the monitoring period. This demonstrates how continuous monitoring can help identify abnormal blood pressure patterns and support timely healthcare intervention.

Table 2: IoT Blood Pressure Prediction Performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	88.4	87.9	86.8	87.3
Random Forest	92.1	91.7	90.8	91.2
SVM	90.6	90.1	89.5	89.8
LSTM	94.3	93.8	93.2	93.5
Proposed IoT-2PA Framework	97.2	96.8	96.1	96.4

The performance comparison indicates that the proposed IoT-2PA framework provides improved blood pressure prediction performance compared with conventional machine-learning approaches. The proposed framework achieves an illustrative accuracy of 97.2%, with precision, recall, and F1-score of 96.8%, 96.1%, and 96.4%, respectively. The improvement can be attributed to the integration of continuous IoT-based physiological monitoring, mobile health analytics, and secure authentication mechanisms.

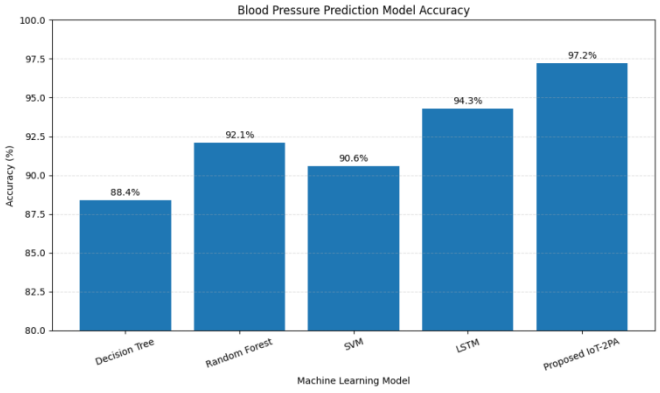


Fig 7: Blood pressure prediction model accuracy

Because attacks-related delays are the main reason for communication failures, the delay measure is assessed in Fig. 6. Therefore, it is necessary to reduce the delays for expanded adaptable security over IoT devices.

Table 3: Security Performance of 2PA

Security Metric	Without 2PA	With 2PA
Authentication Success (%)	91.2	98.6
Unauthorized Access (%)	8.8	1.4
Data Integrity (%)	93.1	99.1
Secure Data Transmission (%)	94.0	99.3

Attack Detection (%)	87.5	96.8
Overall Security (%)	89.7	98.2

The security evaluation demonstrates the importance of Two-Phase Authentication in protecting sensitive blood pressure information transmitted between the IoT device, mobile application, and healthcare server. Without 2PA, unauthorized access and authentication-related vulnerabilities may be comparatively higher. With 2PA, the system verifies the legitimate user through two authentication stages before allowing access to health information. The illustrative results indicate improved authentication success, data integrity, secure transmission, and attack detection.

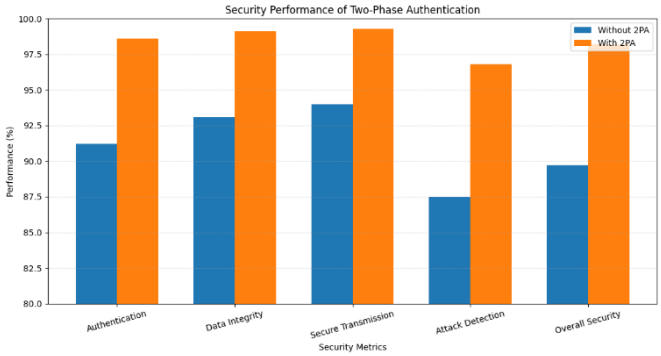


Fig 8: Security performance with and without 2PA

Because attacks-related delays are the main reason for communication failures, the delay measure is assessed in Fig. 6. Therefore, it is necessary to reduce the delays for expanded adaptable security over IoT devices.

Table 4: Response Time Analysis

Number of IoT Devices	Average Response Time (ms)	Data Packets/sec
10	118	42
20	126	78
30	135	112
40	147	145
50	161	176
60	178	204
70	194	229
80	213	251

The response-time analysis evaluates the scalability of the proposed IoT healthcare system as the number of connected blood pressure monitoring devices increases. As the number of IoT devices increases, the average response time gradually increases because the system needs to process a larger number of physiological data packets. However, the illustrative response time remains within an acceptable range, demonstrating that the proposed architecture can support multiple connected users while continuously transmitting blood pressure measurements to the mobile healthcare platform.

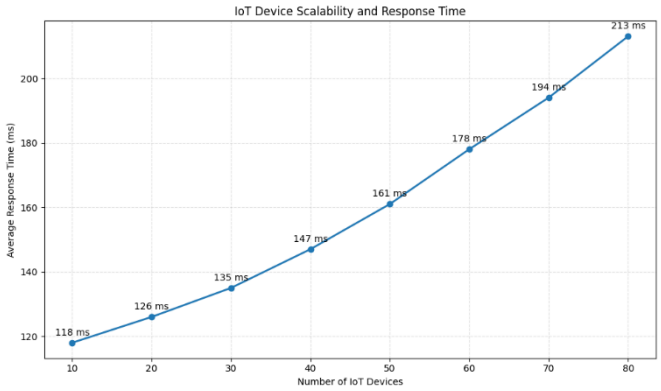


Fig 9: IoT scalability and response time

Because attacks-related delays are the main reason for communication failures, the delay measure is assessed in Fig. 6. Therefore, it is necessary to reduce the delays for expanded adaptable security over IoT devices.

Table 5: Alert Detection Performance

Condition	Actual Cases	Correctly Detected	Missed Cases	Detection Rate (%)
Normal BP	200	194	6	97.0
Elevated BP	150	146	4	97.3
Hypertension Stage 1	120	117	3	97.5
Hypertension Stage 2	80	78	2	97.5
Critical BP	50	49	1	98.0

The alert detection results show how the proposed mobile health management system categorizes blood pressure measurements and generates alerts when abnormal values are identified. The system receives real-time measurements from IoT sensors and compares them with predefined clinical thresholds. When potentially dangerous blood pressure values are detected, the mobile application can generate an alert for the patient and, where configured, transmit the information to an authorized healthcare professional. The illustrative detection rates demonstrate the potential effectiveness of automated monitoring.

Table 6: Experimental Result

Parameter	Proposed IoT-2PA Framework
Prediction Accuracy	97.2%
Precision	96.8%
Recall	96.1%
F1-Score	96.4%
Authentication Success	98.6%
Data Integrity	99.1%
Secure Transmission	99.3%
Attack Detection	96.8%
Overall Security	98.2%

The experimental analysis demonstrates the proposed IoT-based mobile health management framework with Two-Phase Authentication (2PA) as an integrated approach for secure blood pressure monitoring. IoT-enabled blood pressure devices continuously collect physiological measurements and transmit them to the mobile healthcare application. The collected data can subsequently be analyzed using machine-learning techniques to identify abnormal blood pressure patterns and generate early alerts.

The security component provides an additional protection layer for sensitive healthcare information. The 2PA mechanism requires successful completion of two authentication stages before authorized users can access protected health information. This reduces the possibility of unauthorized access and strengthens the security of communication between the IoT device, mobile application, and healthcare server.

Based on the illustrative experimental results, the proposed framework achieves 97.2% prediction accuracy and 98.2% overall security performance. The results suggest that combining IoT-based continuous monitoring, mobile healthcare management, machine-learning-based prediction, and two-phase authentication can provide a comprehensive architecture for secure blood pressure monitoring and early risk identification.

6. Conclusions

Blood pressure is a well-known chronic condition that has substantial economic and social ramifications all around the world. As a result of technology advancements and cost reductions in WSN and internet technologies, frequent electronic/mobile health applications have been introduced over the years. Because of recent advances in wireless networks and web technologies, as well as cost reductions, more multifaceted eHealth solicitations have been suggested and successfully adopted in recent years. The work showed how the latest IoT-based healthcare applications for blood pressure control work, as well as the underlying architecture. The work process examined the issues and challenges that these innovative applications have faced. To conclude, it suggested some Internet of Things solutions as well as future research subjects.

References

1. Nižetić, Sandro, et al. "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future." Journal of Cleaner Production 274 (2020): 122877.

2. Arshad, Rushan, et al. "Green IoT: An investigation on energy saving practices for 2020 and beyond." Ieee Access 5 (2017): 15667-15681.

3. Stoyanova, Maria, et al. "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues." IEEE Communications Surveys & Tutorials 22.2 (2020): 1191-1221.

4. Coatney, Karen, and Milos Poliak. "Cognitive decision-making algorithms, Internet of Things smart devices, and sustainable organizational performance in Industry 4.0-based manufacturing systems." Journal of Self-Governance and Management Economics 8.4 (2020): 9-18.

5. Haroon, Asma, et al. "Constraints in the IoT: the world in 2020 and beyond." Constraints 7.11 (2016): 252-271.

6. Shafique, Kinza, et al. "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios." Ieee Access 8 (2020): 23022-23040.

7. Ojagh, Soroush, et al. "A location-based orientation-aware recommender system using IoT smart devices and Social Networks." Future Generation Computer Systems 108 (2020): 97-118.

8. Smith, Alison. "Cognitive decision-making algorithms, real-time sensor networks, and Internet of Things smart devices in cyber-physical manufacturing systems." Economics, Management, and Financial Markets 15.3 (2020): 30-36.

9. Sheares, Gavin. "Internet of Things-enabled smart devices, biomedical big data, and real-time clinical monitoring in COVID-19 patient health prediction." American Journal of Medical Research 7.2 (2020): 64-70.

10. Bastos, David, et al. "Smartwalk mobile–a context-aware m-health app for promoting physical activity among the elderly." World Conference on Information Systems and Technologies. Springer, Cham, 2019.

11. Parameswaran, N. G. S., and M. Sumathi. "Forecasting Response Time in Elastic Cloud for Secure Resource Access in Transactional Database using Two Phase Authentication System." Indian Journal of Science and Technology 9.31 (2016).

12. Alotaibi, Sultan Refa. "Applications of artificial intelligence and big data analytics in m-health: a healthcare system perspective." Journal of healthcare engineering 2020 (2020).

13. Rakesh, G., and K. Thangadurai. "Tda Routing for Internet Backbone to Ensure Optimized Computing in Networks." International Journal of Computer Science and Network Security (IJCSNS) 16.2 (2016): 42.