S. *et al.*
Journal of Engineering and Applied Science (2024) 71:128
https://doi.org/10.1186/s44147-024-00460-4

Journal of Engineering and Applied Science

RESEARCH Open Access

Achieving Secured Medical Network (SMN) through Stateless Mechanism and SkeyM in Medical-Internet of Things (M-IoT)

Nithya S.[1], SatheeshKumar Palanisamy[2*] and Nivethitha T.[3]

*Correspondence:
satheeshp@bmsit.in

[1] Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamil Nadu 641049, India
[2] Department of Electronics and Communication Engineering, BMS Institute of Technology and Management, Bengaluru, Karnataka 560064, India
[3] Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu 641202, India

Abstract

Medical Internet of Things (M-IoT) synchronizes medical devices in a network to provide smart healthcare monitoring to doctors and to provide an interactive model for patients. This embedded networked system gained lots of importance in the last few years. Now almost every hospital adopts M-IoT. Though it had a lot of challenges in the initial stages of implementation such as feasibility, accuracy, and autonomy, now it has bridged the flaws with the help of several researchers in this field. But still, M-IoT lags behind in security and privacy aspects due to which attackers can intrude on the network and exploit patients' health data. By examining the various intensive security threats imposed on M-IoT a unique way of handling and transferring data over the network is proposed in this paper. From our research findings, this would resolve the data security issues in M-IoT and commence the next advancements.

Keywords: Medical Internet of Things, Medical Data Privacy, Medical network, Key management, Stateless mechanism

Introduction

The information sharing between physical space is called cyber-physical systems, which can be possible only because of the Internet of Things. In other words, can say as the request-response relationship between physical space (sensors, computers, etc.) and information space is called cyber-physical systems (CPS). Cyber-Physical system plays [1]. a vital role in many fields such as vehicular, smart grid, health care, air force, and many others. The application of CPS in the medical field is referred to as Medical CPS (MCPS) or M-IoT [2]. This era of artificial intelligence and advancements lifted Medical-IoT usage and broadened the space for various fields to adopt it. Medical-IoT leaves an enormous amount of footprint in the field of medical and healthcare science, which includes smart operating rooms, Auto monitoring of patients [3], alertness in case of emergency, control of drug flow, etc. In all these synergies, patient data is the only and most critical thing that the technology stack should uphold and process. Several biometric-based authentication [4] and passwordless mechanisms [5] are being floated in the market to protect patient data.

In the case of an authentication system, credentials such as password word, thumb impression, and face recognition are stored locally or remotely. It raises the chances of cyberpunks gaining access to the rights. A stateless mechanism [6] is vital for overcoming this.

A sort of authentication mechanism known as stateless authentication does not require the server to keep track of client context or session state in between requests. Rather, every request made by the client must include all the data required for client authentication and request authorization. Web apps and APIs that make use of token-based authentication protocols like JSON Web Tokens (JWT) [7] or OAuth2 frequently employ stateless authentication. According to this method, the client includes a token with each request that contains the data the server needs to confirm the client's identity and determine whether the client is authorized to access the resource. Stateless authentication can increase scalability and decrease server load because it does not require the server to retain the session state. To ensure the security of the authentication system and guard against attacks like token theft or replay attacks, it also needs to be implemented carefully. Table 1 gives a detailed comparison of the stateful mechanism and stateless mechanism.

The market potential for Medical-IoT devices saw significant growth across different sectors between 2017 and 2022. In 2017, implanted devices were valued at $5.1 billion, and wearable external devices were worth $4.1 billion. By 2022, these values skyrocketed, with implanted devices reaching $18.9 billion and wearable external devices hitting $16.3 billion. This substantial expansion underscores the increasing integration and adoption of IoT technologies across various medical device categories over the 5-year period.

Certainly, several factors influence the adoption of Medical-IoT (Internet of Things) in the healthcare sector.

- Ensuring close monitoring of patients who are bedridden is crucial. In order to provide patients with the best care possible, nurses and doctors greatly benefit from

Table 1 Comparision of stateful and stateless authentication mechanism

Metrics to compare	Stateful	Stateless
Session information could be stolen	Yes	No
Resource consuming	High	Low
Implementation	Complex, as it required an external database	Easy
scale	Adding new services and instances is not that easy	No additional effort is required to scale up
Possibility to compromise session data	Information about sessions can only be retrieved by the authentication system	All components of the system are in danger if at least one system has been compromised
Authentication token size	Data does not affect its size	Size depends on the size of the data
Possibility to revoke session	Possible	Impossible
Possibility to modify session data	Possible	Impossible
SSO implementation	It is feasible to integrate many system components without changing the source code	Each component has to be changed

wearable and implantable devices. These devices not only monitor any changes in the patient's condition but also provide automated task suggestions, which ease staff assistance. Thus, monitoring these patients via these devices not only ensures their safety but also improves the quality of work that physicians and nurses perform.

- Using complex computer algorithms is like having quick and intelligent assistants. Medical devices equipped with these advanced algorithms can process and organize patient data much faster and more accurately than humans can. This saves a lot of time, especially in emergency situations, allowing healthcare providers to focus more on immediate patient care.
- Remote monitoring is becoming more and more necessary as the population ages and the number of chronic illnesses rises. This involves tracking patients outside of the hospital as well. IoT-enabled stationary medical equipment plays a critical role in addressing this requirement.
- Hospitals manage sensitive patient data, thus privacy and data security are major concerns. Assuring the protection of patient information is essential for regulatory compliance and fostering faith in the technology, adoption may be hindered if hospitals lack confidence in the security mechanisms of M-IoT devices and networks.
- In addition to the factors mentioned above, the adoption of Medical-IoT in the healthcare sector is influenced by decreased error rates resulting from reduced human involvement, improved resource management, and enhanced preventive medicine.

However, security remains the most important worry in the healthcare industry. To maintain a healthy balance between utility and privacy, data analysis with the essential security and privacy-preserving characteristics is required. This type of data analysis that protects privacy enhances efficiency when sharing, managing, and controlling medical data. Every day, there is a greater demand for privacy preservation approaches for web data in order to resolve privacy conflicts, reduce privacy violations, and promote the use of web apps without jeopardizing user privacy. The liquidity of data imposes high concern over security and privacy. Though security is the mainstream for research, still it has a void that deprives the usage of Medical-IoT. Typically, medical/patient data is acquired by numerous sensors and medical devices and saved in massive private storage or in a cloud environment [8]. Data is supposed to go across an open channel in this case, there is a significant possibility of a data breach. To protect data in motion or group data, a strong security method is required. This article focuses on the security aspects of Medical-IoT and derives an end solution for it.

Priority on medical data security

Patient data privacy is one of the most important issues in the healthcare industry. A US survey states that, in 2015 around ten million data breaches had happened in healthcare. Most the hospital fails to secure patient health information (PHI) or electronic health records (EHR) which are collected through Medical-IoTs [9]. Hospitals had to upgrade themselves in technologies to overcome these factors. Several studies have been carried out in order to protect medical images [10]. Healthcare data holds more value than any other data. For example, by comparing credit card

data and healthcare data, if a credit card is lost there is the possibility to change the secured PIN or block the card when a customer approaches the bank. But in the case of PHI, which is permanent and cannot be changeable. They can make fraudulent reports. Every year cyberpunk earns up to $ 100,000 only by stealing health care data. So the security of health care [11] data should be tightened.

Forge walls for Medical-IoT breach

Here are some of the solutions to avoid the Medical-IoT data breach. (i) The corresponding organization should in-phase their own infra network, and without stopping in it, they should upgrade their systems periodically. (ii) Maintain PHI across the multi-server tenants. (iii) Backup the important data to the backend server and scrap the exposed servers periodically. (iv) Entire hospital employees who are involved in protecting PHI or EHR to be updated in all kinds of attacks in M-IoT. (iv) One of the best ways is to develop an internal data protection policy and regulate them to adopt their policy. (v) It is also important to monitor the external hacker by conducting orbital physical checks on camera records and servers.

Health care industry gives us more priority to improve their Medical-IoT devices such as MRI, Medical Image [12], and scanning devices instead of building a better and safer network. However, the network plays a major role in protecting patient data. Patient privacy should be preserved like the assert of an organization. This proposed system focuses on how to protect the patient health information collected through M-IoT from cyberpunk in order to achieve patient safety.

Implementing IoT in healthcare can indeed be a significant challenge, especially regarding data security. The extensive network of heterogeneous medical devices increases the risk of device hacking. With a wide range of devices, each device becomes a potential entry point for hackers. Implementing a unique and complex authentication mechanism for each device enhances security by limiting unauthorized access. While this article has already proposed unique and strong mechanisms to address security concerns, there are several other challenges that need to be taken care of. Let us look at how these issues are being addressed.

The National Institutes of Health highlighted three primary factors influencing the data quality of wearable devices. As the reviewer addressed, user error is one such factor that needs crucial consideration. This challenge can be addressed by implementing advanced machine learning algorithms, such as fuzzy algorithms, to analyze and observe user behavior. These algorithms are capable of processing large volumes of data collected from wearable devices and identifying deviations or anomalies from normal behavior. In such algorithms, true abnormalities can be accurately identified, distinguishing them from false positives. True abnormalities can then be promptly communicated to the user or caregiver, enabling timely intervention. Meanwhile, false positives can be flagged as outliers.

Furthermore, companies like Apple are at the forefront of incorporating abnormal motion/activity tracking into their wearables.

Related work

Most of the research works have used typical cryptography methods such as encryption and decryption to ensure the security of medical data. The secret key or secure key is shared among the sender and receiver to encrypt or decrypt the data. Securing the data that is transmitted across the IoT network every second is of the utmost importance. Below is a list of some recent studies on data security.

A cloud-based anti-malware system called CloudEyes was suggested by [13]. The proposed strategy offered the IoT network's devices effective and reliable security services. Based on the idea of trusted computing [14], research on embedded security requirements included methods and solutions for fending off cyberattacks as well as technology for tamper-proofing embedded devices. investigates how to securely invoke patients' records from past case databases while protecting the privacy of both currently diagnosed patients and the case database and construct a privacy-preserving medical record searching scheme based on the ElGamal Blind Signature. The advantages of this PMRSS model [15] are bilateral security, adjusting the number of zeros, eliminating the need for doctors, and low latency.

A novel healthcare IoT system has been proposed by [16] which focuses on fusing the advantages of attribute-based encryption, cloud, and edge computing, which provide an efficient, flexible, secure fine-grained access control mechanism with data verification in healthcare IoT networks. Medical files can be encrypted using either attribute-based access or break-glass access, according to the lightweight break-glass access control (LiBAC) method suggested by [17]. In typical circumstances, a medical professional can decrypt data and access it if the attribute set complies with the access policy of a medical file. Emergency medical care providers or rescue personnel can quickly access the data by using a break-glass access mechanism, which can get beyond the medical file's access restrictions, in an emergency.

Frequently the data collected in a healthcare IoT system is vital and sensitive. Therefore, circulated data's integrity, authenticity, and sequestration are abecedarian security demands to end users and possessors. To address these challenges, the authors [18] a featherlight and secure redactable hand scheme with coarse-granulated fresh redaction control (CRS) for secure dispersion of healthcare data in a pall-supported healthcare IoT system is proposed. The security analysis indicates the CRS is secure against hand phony, fresh redaction attacks, and redacted interpretation linkability. Compared to other results, this scheme can achieve some position of security but lower computational complexity and communication outflow. A secure data-sharing system based on KASE in a fog-enabled IoT environment using blockchain is proposed by [19]. Resistance of the proposed scheme against various attacks through informal analysis and Automated Validation of the Internet Security Protocols and Applications (AVISPA) simulation tool is proved along with the guarantee of secure mutual authentication using Burrows-Abadi-Needham (BAN) logic.

To conceal message bits, [20] suggested using H.264/AVC's flexible macro-block ordering (FMO) feature. The content of the message bits that are to be masked is used to determine which slice groups the macroblocks are allocated to. A maximum payload of three message bits per macroblock is accomplished using the suggested technique.

A reversible perturbation technique with access control was put into practice by [21]. For each level, a dataset snapshot is made available. Multi-level access is provided using perturbation keys. We need a sizable bipartite association graph dataset. The nodes and edges in the graph are permuted in this method to secure the information. This method results in an additional overhead because it uses perturbation keys to offer snapshots of the rebuilt data.

Palanisamy [22] presented a combination method using perturbation and clustering. Healthcare information that has been disturbed is accessible on the cloud and is mined. The geometric data perturbation (GDP) method guards against unauthorized access from outside parties. By keeping the disturbed data in the public cloud and its matching keys in the private cloud, the storage is improved. The selection of clusters is crucial for organizing and safeguarding the data.

Qi et al. [23] illustrated a model for strengthening the security of encryption and decryption in medical images. In elliptic curve cryptography, the optimal key will be chosen using hybrid swarm optimization, which combines grasshopper and particle swarm optimization. The medical images are safeguarded in the IoT framework using this way. Khari et al. [24] examined traditional and emerging encryption techniques in terms of their capacity to provide secure storage, data sharing, and computing. Because each layer's hardware and communication capabilities change, separate encryption algorithms must be utilized to ensure data privacy inside that layer. Sun et al. [25] suggested a strong and inexpensive picture encryption solution for the healthcare business that uses permutation algorithms to secure medical images. The key benefit of this strategy is that it is not application-specific. Most rich countries employ Telecare Medicine Information Systems (TMIS) to assist patients. To prevent misuse, patient data must be secured. An effective and secure system using biometric-based authentication and a key agreements protocol was proposed [4]. The three steps of the proposed system are the registration phase, the login phase, and the key agreement phase. The system was subjected to many security attacks for analysis. The system was examined using different security attacks and determined to be impenetrable to all of them. Along with the other medical data, user identification is likewise secured.

The authentication and key relay mechanism [26] were used to ensure medical data security. In this method, the secure key is used to achieve authentication, confidentiality, data freshness, and integrity. Authentication allows the caregiver or patient to ensure that the data really comes from the right person. Confidentiality is used to disclose medical data from unauthorized persons. Integrity ensures the data are valid, i.e., prevents unauthorized people from altering the data. Data freshness ensures no man-in-middle attack was happening. To ensure medical image security [27] watermarking was adopted, in this method, the original medical images such as CT scans, and ECG images were watermarked by using ROI (region of interest), and then by extracting we can get the original images. Medical images were securely transferred as watermarked images over a medical network [27] to attempt to overcome difficulties associated with biometric-based authentication systems, such as user impersonation. As a solution, the author used a secure three-factor authentication architecture that is more appropriate for a practical scenario. Integrating a chi-square detector and a Fuzzy logic-based attack classifier [28] presented a method for identifying distributed denial of service and false data

injection attacks. The suggested approach surpasses the traditional distributed denial of service and false data detectors.

Oh et al. [2] studied extremely secure medical images with the use of subkeys, first by employing chaotic logistic and tent maps with a handful of subkeys. The chaotic (C-function) process was used to explore security issues such as diffusion and confusion. Different random numbers were generated for each chaotic map based on the initial conditions. To select the ideal secret and public key [29] of the system from a set of random numbers, an adaptive grasshopper optimization algorithm with PSNR and correlation coefficient fitness function was proposed. Hasan et al. [10] proposed a signal temporal logic (STL)-based approach to observe typical system activity. Anomalies are defined as trajectory deviations from the learned formula. Can also be utilized for anomaly mitigation via formal synthesis and early detection via online monitoring.

Cryptography and steganography techniques are essential for IoT security, and the [30] proposed work uses an elliptic Galois cryptography protocol to encrypt confidential data and embed it into a low-complexity image. and approximately 86% steganography embedding efficiency was achieved. Results from this proposed protocol were compared to existing methods, such as OMME, FMO, and LSB. Novel mathematical methods [31] for identifying anomalous traffic in large-scale data networks. The static configuration analysis and dynamic traffic analytics are combined in this. Security settings are used to statically check for potential security vulnerabilities such as violations of network-wide invariants. Then, create dynamic data analytic algorithms to examine real-time traffic and detect aberrant traffic patterns that may be exploiting network security vulnerabilities.

The WBAN (wireless body area network) authentication mechanism [32] was developed to identify the unauthorized node in the medical network. In this process, only authorized nodes can be a part of the medical network. The WBAN authentication method will identify a bad node and reject it. This will help to improve the reliability and security of medical data that is traveling around the medical network.

The behavior specification method [33] is also used to ensure the security of medical data. Each entity of the medical network was kept on the monitor, if there is any deviation from specified behavior, automatically that particular entity will be identified as an intrusion. Figure 1 explains the above method.

If there is any new behavior is identified in the network that is actually not harmful it automatically adds to behavioral rule using machine learning techniques in order to avoid false positives, this is called “self-learning” of states.

Reddy and Rao [34] proposed an intelligent sensing approach that intentionally generates incorrect data to attract atypical users. A fair play point approach is used to identify abnormalities. The proposed approach has a maximum accuracy of 99.2%, which is 25.1% higher than the SVM-RBF. Caruso et al. [35] creates a dynamic attack detector that identifies observable attacks which includes defined attacks that can go on indefinitely without being discovered. Then define the zero state-producing attack, which is the only sort of attack that stays dynamically undetectable regardless of the side beginning state information accessible to the attack detector.

In the Industrial Internet of Things, a dynamic wireless sensor network is crucial (IIoT). Key management is easily manipulated because of its dynamic nature due to a

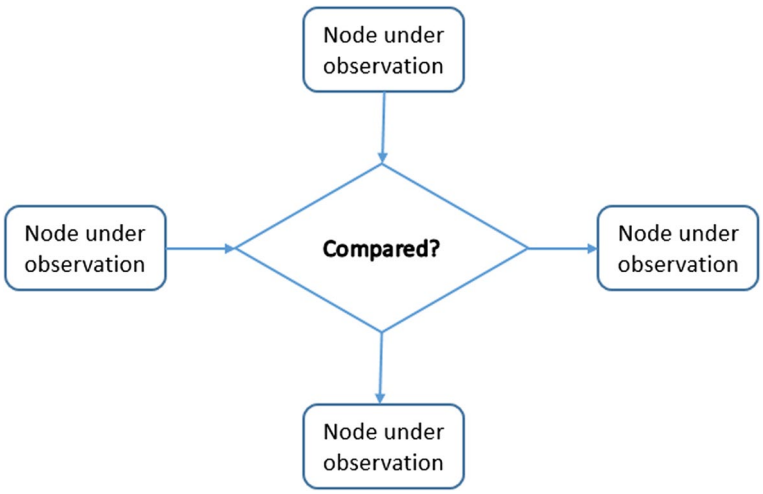

Fig. 1 Behavior specification method of medical nodes

hacked base station. Suganya [36] suggested a blockchain-based secure key management method (BC-EKM) that does the majority of the base station work in order to prevent this. The blockchain system maintains a secured database and serves as a secured trust machine. Node registration, cluster creation, node motion, and guilty node detection make up BC-EKM. The proposed system's principal objective is to establish credibility.

When transferred to distant entities, medical information about the patient must be protected. Abdmeziem and Tandjaoui [37] created an energy-aware key management system to offer end-to-end encryption. In the proposed work, a channel is created to enable communication from highly resourced nodes to a remote entity. If any high-end information is found, it is given to a third party so that a powerful entity can access it. During the communication, the channel should ensure authenticity and privacy.

Methods/experimental

The Internet of Medical Things (IoMT) is a rising trend that provides a significant quantum of effective and effective services for cases as well as healthcare professionals for the treatment of distant conditions. The lack of security mindfulness among neophyte IoMT users and the threat of several central attacks for penetrating health information oppressively jeopardize the use of IoMT.

Traditional encryption solutions cannot be employed directly to e-health data reasons of data size constraints, redundancy, and capacity, particularly when patient data is sent via open channels. To overcome these security concerns, a strong security mechanism is required.

Aim

This paper aims to eliminate the drawbacks of server-side authentication [23] of the users and encryption strategies in protecting the data through a stateless mechanism called SkeyM (strapping key management) in which the user data is never ever stored in the server memory. All authentication process takes place in the workflows and the SkeyM algorithm generates a unique token based on a highly complex secret key and

sends the token to the user. This secret key is unique for every token generated and only the server knows about the secret key. It is never transmitted over the network, thus assuring a stateless mechanism. The user sends the query with the SkeyM token signed in. The server upon receiving the query, decouples the SkeyM token to match with the secret key and process the query. In this same way, all the communication happens between the M-IoT and the server. So nowhere the data from M-IoT devices nor the mechanism for decoupling the token is shared over the network. Algorithm 1 explains the working of the SkeyM authentication Technique.

Algorithm 1 SkeyM algorithm

Input: *Creditial from Doctor(C_i), Token generated by stateless server (T_{ss})*
Output : *Complex unique SkeyM token ($T_{skey}M$)*
1:(X) Input: C_i
2: (Y) Input: T_{ss}
3: if (C_i == T_{ss})
4:Generate $T_{skey}M$
5: raise Req_i for P_i ,along with $T_{skey}M$
: Receive Res_i
7: $T_{skey}M$ Expire
8: Repeat 1 to 7 for another request
9: ***else***
10: ***return Fail***

The server's job is only to create a unique secret key, make validations using tokens, and process the requests. All the tokens are embedded with an expiry time. Upon expiry, the user had to re-login and generate a new token request. This expiry of tokens helps to overcome major attacks which will be discussed in later headings. In experimental analysis, the proposed methodologies attain better results than the prevailing styles.

Design and workflow

This authentication system after validating the credentials passes an identifier flag to the data server to generate a secret key that is unique for this user login and creates a corresponding token that has a signature for the data transfer and expiration time. This token is transferred to the user with the acknowledgment. The user when making a request, that query is signed up with the token and sent to the server. The server on receiving the query, decouples the token and verifies it with the secret key. If matches happen then the query is processed and again data is embedded with the token and transmitted over the network. In this way, communication happens between the user and the data server.

After the expiry of the token, the user will be re-authenticated and a new token will be generated for further requests. This token regeneration is completely abstracted from the user, so their task is all about their requests. In the whole workflow, nowhere the user data is transmitted, so the attackers will not get any chance to authenticate with the system. The same has been depicted in Fig. 2.

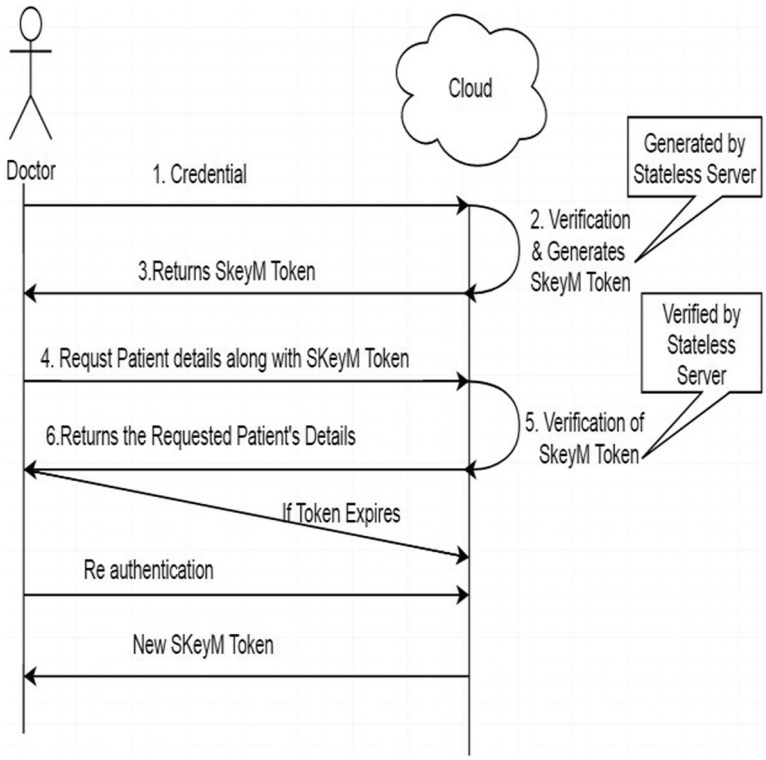

Fig. 2 Workflow of SkeyM authentication method

Doctor nodes and medical devices (user nodes) deployed as workloads on AWS virtual machines communicate securely using SKEYM tokens. When a request is made from the Doctor node to the user node, it is verified, and a unique SKEYM token is generated to ensure the authenticity of the nodes in the network. All communication between the nodes occurs using this SKEYM token. If the token expires, the node regenerates a new token for further communication. To test the strength of the proposed mechanism, intentional attacks are launched from attacker nodes deployed in the cloud. However, it takes approximately 10 to 15 h to crack the token with a length of 128 bits, but the token expires before it can be cracked. This illustrates how the mechanism effectively ensures secure communication between nodes and prevents potential attacks from malicious actors.

Experimental setting of the study

Stateless mechanism and SkeyM for secured medical networks (SMN) in M-IoT [24]. This analysis delves into the approach of using a stateless mechanism and SkeyM (symmetric key management scheme) to achieve a secure medical network (SMN) in the context of the Medical Internet of Things (M-IoT). It will compare this approach with recent advancements in M-IoT security.

Strengths of the stateless mechanism and SkeyM approach [29]

Scalability and efficiency: stateless protocols eliminate the need to maintain session state, making them ideal for resource-constrained M-IoT devices. This translates to better scalability and lower processing overhead compared to stateful mechanisms.

Security benefits of SkeyM

Secure key distribution [21]

SkeyM facilitates the secure distribution of cryptographic keys to various M-IoT devices within the network.

Dynamic key management [18]

SkeyM allows for efficient key updates and revocation, crucial for dynamic M-IoT environments where devices may be added, removed, or compromised.

Comparison with recent literature

Lightweight authentication protocols [11] Research in M-IoT security has emphasized lightweight authentication protocols due to device limitations. Compare the efficiency and security guarantees of the stateless mechanism with recent proposals in this area.

Alternative key management schemes While SkeyM offers secure key management, explore recent literature on alternative schemes like identity-based encryption (IBE) or attribute-based encryption (ABE) [4]. These schemes offer additional security features, such as fine-grained access control, which might be relevant depending on the specific SMN requirements. Analyze recent research on SMN security, particularly focusing on:

- Lightweight authentication and key agreement protocols specifically designed for M-IoT.
- Secure communication mechanisms that ensure data confidentiality and integrity during transmission within the M-IoT network.
- Privacy-preserving data aggregation techniques that enable efficient data collection from various M-IoT devices while protecting patient privacy.

Benefits

There are a range of unstoppable fortunes which made to prefer it. Following are some of the glimpses.

Security metrics

Considering security as the main concern, this token generation is designed. The secret key and expiration play a crucial role. The token generated using the SkeyM algorithm will be unique on each authentication, so it is highly difficult for malicious nodes to find the token within the expiration time. The secret key will only reside on the server and it is not transmitted in any request to the user. The server on fetching back the token, decouples with the secret key and makes matches and only if it succeeds, the corresponding request will be processed and transmitted encrypted JSON data. The expired token fails at the security layer and has no need for processing [38].

Unknown source

These are stateless. The server is completely unaware of the user who sends the request. The user's information is never ever cached in the server's memory. The server can validate the token locally without making any network requests. So that even when a third party tries to access the token, no data other than the username will be revealed.

No history of sessions

Usually, the user requests will be stored as a cache, and garbage collected after the session ends. But in our case, at the security layer itself expiry time is checked and the token will be refused access. This reduces the overhead of garbage collection.

User-centric design

One of the standout features of this method is its fully automated key generation process. This automation eliminates the need for users to manually generate keys, significantly simplifying their experience. Instead, users are only required to attach the automatically generated key along with their request. The verification of these keys is seamlessly handled by serverless functions, relieving users of the burden of manual verification processes. Moreover, the utilization of serverless architecture adds another layer of efficiency to the system.

Being serverless means that the infrastructure required to support the system is lightweight and dynamically scalable, optimizing resource utilization and minimizing operational overhead. This translates to a more agile and cost-effective solution, without compromising on security or performance.

The strength of this approach lies in its user-centric design. By streamlining complex cryptographic processes and leveraging serverless technology, the system ensures that even users with limited technical expertise can effortlessly participate in secure transactions. This simplicity, coupled with robust security measures, makes the proposed method a standout choice in today's cyber world.

Scalability concerns

Scalability is indeed a crucial factor in network design, particularly in medical networks where critical nodes are interconnected. To tackle this challenge, Medical-IoT systems are crafted with flexible architectures capable of accommodating an expanding array of devices and users. By embracing cloud computing platforms, healthcare organizations can dynamically scale their Medical-IoT infrastructure to meet evolving needs.

Furthermore, the proposed token mechanism is exceptionally lightweight, making it seamlessly adaptable to cloud environments. This lightweight nature ensures that the system can efficiently scale up or down as requested, without compromising performance or security.

Thus, by combining flexible architectures with cloud-based solutions and lightweight mechanisms, medical networks can effectively address scalability concerns and support the seamless growth of IoT ecosystems in healthcare settings.

Long-term maintenance

Maintenance is crucial for ensuring the lifespan and reliability of a medical network, especially considering the critical data it handles. Regular software and hardware updates are essential to patch security vulnerabilities, improve performance, and ensure compatibility with evolving technologies. However, it is equally important that these updates are handled by authenticated parties only to maintain the integrity and security of the network.

Allowing unauthorized parties to access and maintain the medical network can ruin its security. This can be achieved through robust authentication mechanisms, such as multi-factor authentication or role-based access control.

Any medical devices require regular security audits, continuous monitoring, and proactive measures to mitigate risks. By addressing this aspect as future or extended work, we ensure that security remains a top priority and that the ecosystem of the medical network is safeguarded against potential risks and threats.

Proof inspections

To prove the standalone architecture of SkeyM, various inspections were carried out with different attacking methods, and below are a few glimpses of it. The main focus of these test cases was to evaluate the key and time expiration features of SkeyM.

Brute force attack

Most of the network attacks will be comprised of brute force attacks. So to test the complexity of the SkeyM token, we tried to brute force the keys. Brute force scripts ran for hours to match the key but all those went to bins. We went even one step further to test against brute force by matching with sampling keys. We generated around 10 million sample keys and attempted to match them. The same scenario has been repeated for several sequences. In all the sequences, none of the tokens were matched. This proves the uniqueness of the SkeyM methodology. The fruit lies in the algorithm that generates the key. The main aim of attackers will be to hack the key so that further requests can be made to the server with that key. In our case, accessing the SkeyM key itself is an intricate task. The following table projects the results of brute force attacks on various weak keys and our SkeyM keys. Table 2 gives the details of the time taken to crack the various types of tokens, and also we can infer that the proposed method will take a longer time to crack. The same has been picturized in the Figs. 3 and 4.

Figure 5 Explains the Brute Force attack on this SkeyM has been attempted for 22 h and the prediction was only 32 bits degradation. This is evident in the complex structure of key design

Timing attack

Timing attacks exploits information leaked from channels during the delays between the requests. To find whether this timing attack will be a threat to our SKeyM methodology, experiments were conducted. Delay between the user requests is the major key character which timing attack relies.

Table 2 Time taken to crack the various types of keys

Type of token keys	Bit length	Time taken to crack
Sequential	32	7 se
	64	6 min
	128	24 min
	256	1.2 h
Dictionary	32	3 h 54 min
	64	5 h 16 min
	128	8 h 42 min
	256	13 h
SkeyM	128	13 h
	256	21 h
	320	More than 31 h

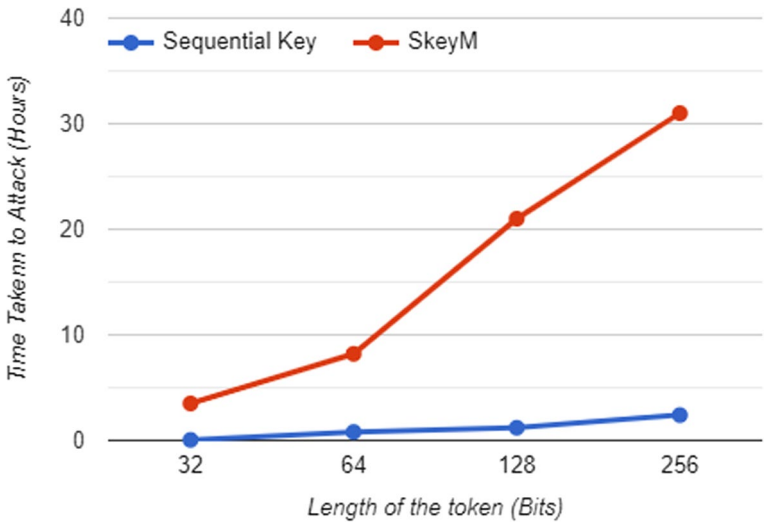

Fig. 3 Time taken to attack SkeyM and sequential keys

Major difficulty is the number of requests a potential attacker needs to find the bytes. Following example demonstrates the use case. To find the first byte of the token, it has to make 128 million requests. To find all 256 bits of the token, 4096 million requests in total. Suppose consider the DDoS could send 50 requests/second, then the attack would take 22 h to find the token. But the SkeyM tokens have an expiry of less than a minute. For further requests, a new token will be used. So, it is easy to pull off. Figure 6 shows the timing attacks for various lengths of tokens.

Processing time

There are numerous machine learning algorithms available to generate secure tokens, such as the subkey generation approach and Neural Key Generation [39], which will aid in the detection of risks disguised behind encryption. However, in this method, a large amount of data must be trained and tested in order to produce the optimal solution. Machine learning and deep learning [40] make it very difficult to cope with the new data that comes at

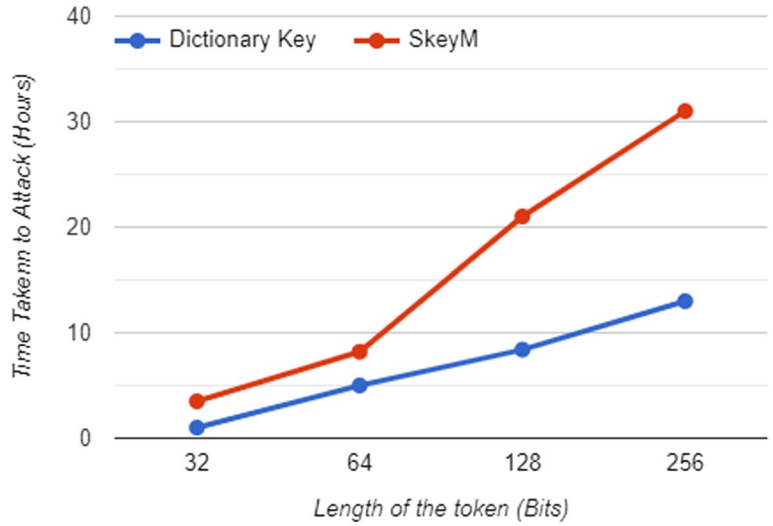

Fig. 4 Time taken to attack SkeyM and dictionary keys

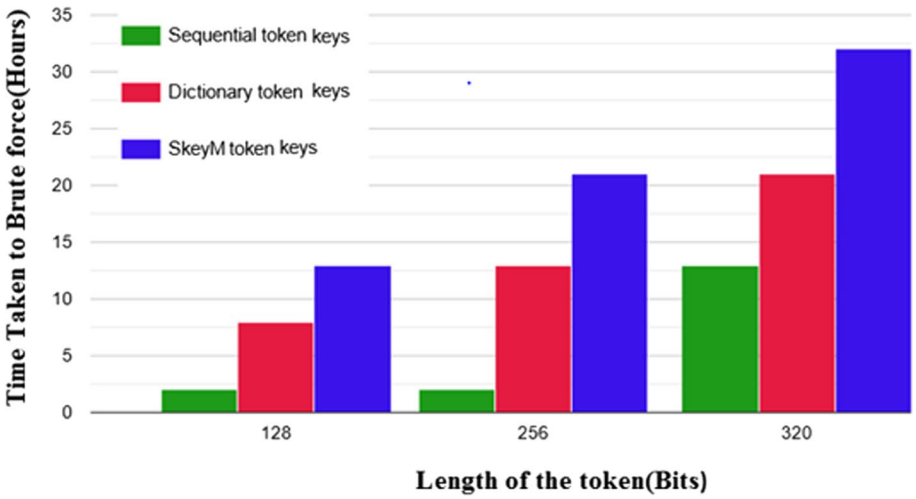

Fig. 5 Comparsion of Time taken to attck

lightning speed, so the data becomes old every day as new data comes machine learning can learn new data based on a training set but it does not produce the expected accurate result. In contrast, this stateless technique requires extremely little effort to provide security and very little storage capacity. Multiple types of key generation methods [41] are compared with the SKeyM Authentication method with various parameters [42], the same has been depicted in Table 3 and Fig. 7.

Results and discussion

Most of the secure key methods in the market are vulnerable to collision attacks because they cannot sign large data efficiently. But this SKeyM methodology is architected in a way that it has a minimum probability of collision of two keys [43] with no hypothesis. Let us conclude it with proof of inspection.

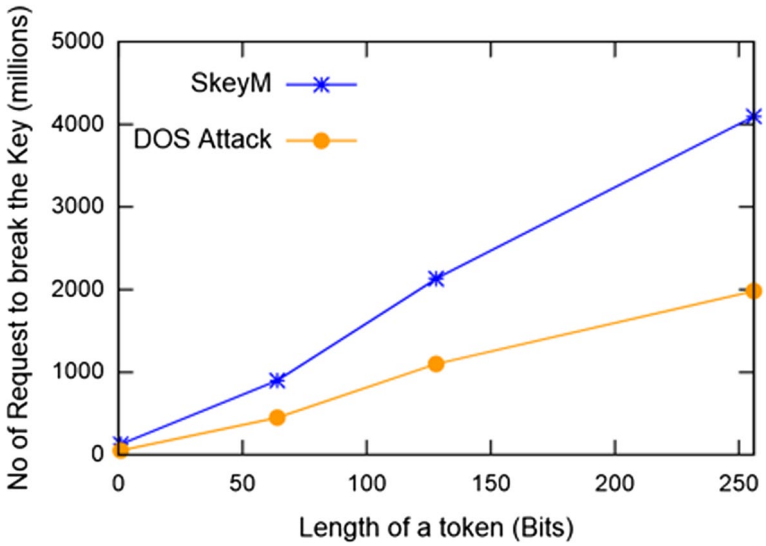

Fig. 6 Timing attack for various lengths of tokens

Table 3 Comparision of SKeyM mechanism with various key generation methods

	Subkey generation approach	Neural key generation	SKeyM key mechanism
Key generation time	1.2 ms	0.8 ms	0.001 ms
Time taken to attack the key	8 h	13 h	More than 31 h
Length of the support	256 bits	256 bits	320 bits

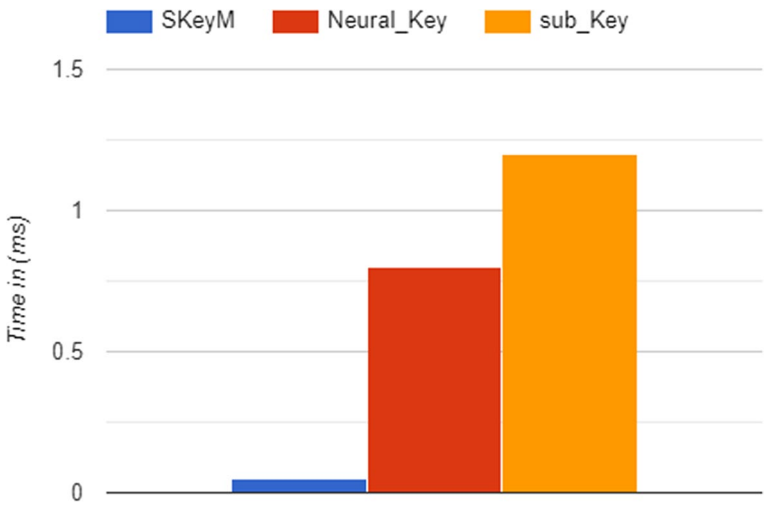

Fig. 7 Key generation time

Let p_n be the probability of collision of n number of distinct keys to k possible values then probability will be

$$p_n = 1 - q_n = \frac{k!}{(k-n)!k^n} \tag{1}$$

For large values of k, $k - n \approx k$.
Using Stirling's approximation, for large values of x,

$$x! = \sqrt{2\pi x}\left(\frac{x}{e}\right)^x \tag{2}$$

On substituting we get

$$q_n \approx \frac{\left(\frac{k}{e}\right)^k}{\left(\frac{\mathrm{k-n}}{\mathrm{e}}\right)^{\mathrm{k-n}}\mathrm{k^n}} = \left(1 - \frac{n}{k}\right)^{n-k} e^{-n} \tag{3}$$

Taking the logarithm of approximation of q_n,

$$\log(q_n) = (n-k)\log\left(1 - \frac{n}{k}\right) - n \approx -\frac{n^2}{2k} \tag{4}$$

Thus arrived at $p_n = 1 - q_n with$

$$q_n \approx e^{-\frac{n^2}{2k}} \text{ (with larger k and } n \ll k) \tag{5}$$

Example
Assuming n as $n = 2^{130}$ distinct inputs with hypothetical values as $k = 2^{256}$ then the probability of collision will be.

$$q_n = -\frac{n^2}{2k} \approx -\frac{\left(2^{130}\right)^2}{\left(2.2^{256}\right)} \tag{6}$$

$$= -2^{2.130-1-256} = -2^3 = -8 \tag{7}$$

So less than 8 chances in a million million millions. And 2^{130} is so large that it is practically impossible to perform that number of operations and match the exact present key within the expiry time. On calculating the probability

$$q_n \approx e^{-8} \approx 0.034\% \tag{8}$$

$$p_n = 1 - q_n \approx 99.966\% \tag{9}$$

The performance metrics such as accuracy, misclassification [44], and the computation time of various privacy methods are measured with SkeyM authentication methods in Table 4.

The accuracy of the SkeyM method is compared with various authentication systems and from Fig. 8 we can observe that the proposed method has a higher accuracy than other methods.

Table 4 Comparision of performance metrics

Various authentication system	Accuracy (%)	Misclassification (%)	Computation time (sec)
FRP-NB	92.3	05.45	2.1
FRP-NB with MFO	93.25	05.08	1.84
FRP-GRNN	94.66	04.90	1.23
FRP-GRNN with MFO	95.42	04.58	1.04
SKeyM	96.71	03.74	0.92

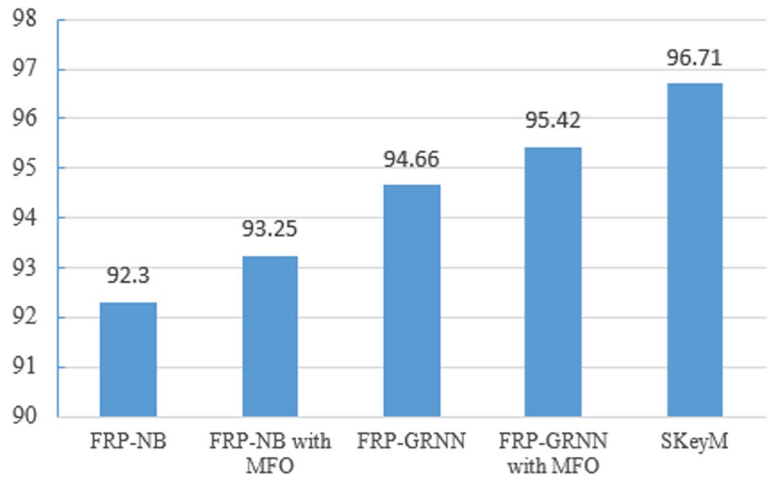

Fig. 8 Comparison of accuracy

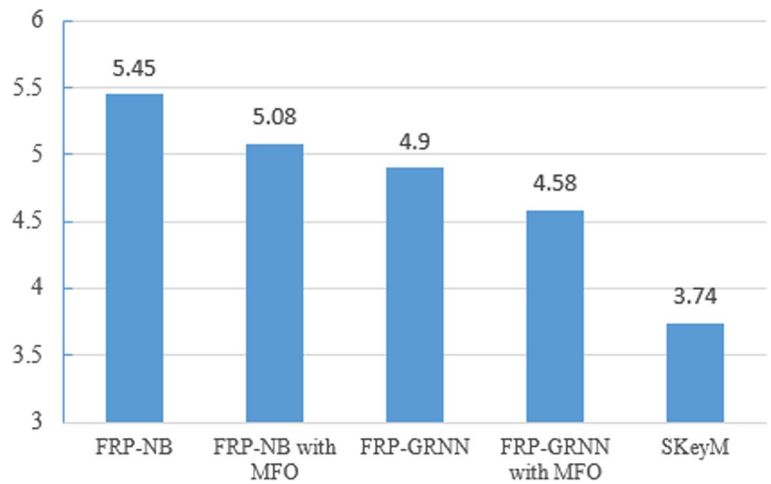

Fig. 9 Comparison of computation time

The computation of the SkeyM method is compared with various authentication systems and from the Fig. 9 we can observe that the proposed method has a lower computation time than other methods.

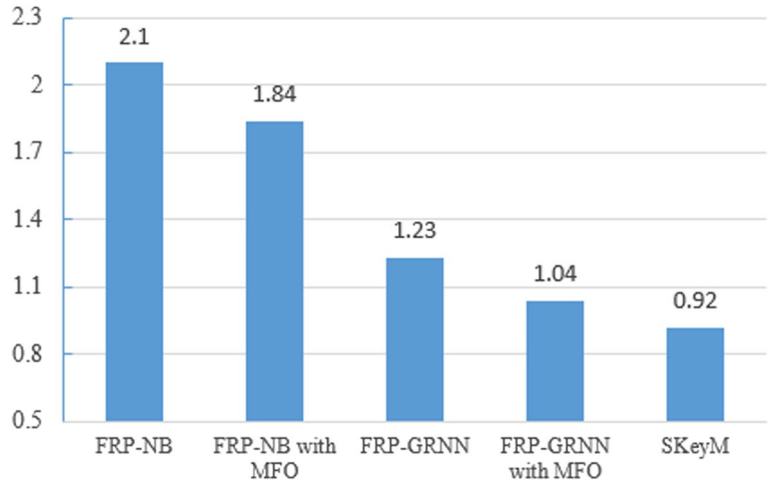

Fig. 10 Comparison of misgenerating of keys

In any key management system, there is a possibility of key misgeneration. These data are compared, and we can conclude from Fig. 10 that the SkeyM technique has a very low likelihood of misgenerating a key.

Conclusions

It is clearly evident from the advent of MCPS in recent years, that the security concepts are so far behind to be focused on. This emphasizes the researchers to work towards comprehensive systems that would really address real-world cyber thefts and protect user's identities. To strengthen this future scope and to shed some light, this white paper positions an innovation called SkeyM methodology which would protect from vulnerabilities by a unique way of token mechanism. The stateless authentication as an add-on would definitely verify the user and not where the user's data or identity will be transferred over the network. We strongly believe that this paper would impact the community security needs and open topics for future contributions. For broader adoption, usability is the key, i.e., complex user interactions can discourage people from adopting the technology. Imagine a doctor needing to perform intricate steps for every interaction with an IoMT device. This can hinder workflow and decrease willingness to use the system. If the system is too complex, it might be difficult to scale its deployment across diverse healthcare settings with varying levels of technical expertise among users.

Also, reduced errors and complicated user interfaces can lead to errors, potentially compromising the integrity and security of the system. Mistakes during authentication or data access could have serious consequences in a healthcare setting.

A user-friendly system allows for faster and more streamlined interactions with IoMT devices. This translates to improved efficiency for healthcare professionals and smoother integration of the technology into their workflow.

In the future, this SkeyM authentication mechanism can be used to carry larger bytes of data. Can also focus on data throughput and structure a prototype along with the SkeyM methodology. The other direction of research will be on implementing medical data analysis to classify and categorize MCPS threats with minimum delay or no delays.

Abbreviations

SMN	Secured medical network
SkeyM	Strapping key management
M-IoT	Medical Internet of Things
MCPS	Medical Cyber-Physical Systems
JWT	JSON Web Tokens
PHI	Patient Health Information
MRI	Magnetic resonance imaging
LiBAC	Lightweight break-glass access control
AVISPA	Automated Validation of the Internet Security Protocols and Applications
BAN	Burrows-Abadi-Needham
TMIS	Telecare Medicine Information System
ECG	Electro-CardioGram
STL	Signal temporal logic
WBAN	Wireless body area network
BC-EKM	Blockchain-based secure key management method

Acknowledgements
Not applicable.

Authors' contributions
Conceptualization: S.Nithya, T.Nivethitha. Data curation: Satheeshkumar Palanisamy. Formal analysis: S.Nithya. Investigation: Satheeshkumar Palanisamy, S.Nithya. Project administration: Satheeshkumar Palanisamy. Resources: S.Nithya, T.Nivethitha
Software, and Validation: Satheeshkumar Palanisamy. Visualization: T.Nivethitha. Writing—original draft: S.Nithya, T.Nivethitha. Writing—review and editing: Satheeshkumar Palanisamy, T.Nivethitha. All authors read and approved the final manuscript.

Funding
Not applicable.

Availability of data and materials
No data is available or generated.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 29 March 2024 Accepted: 28 May 2024
Published online: 10 June 2024

References

1. Sun Y, Liu J, Yu K, Alazab M, Lin K (2021) PMRSS: privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare. IEEE Trans Industr Inf 18(3):1981–1990
2. Oh J, Lee J, Kim M, Park Y, Park K, Noh S (2022) A secure data sharing based on key aggregate searchable encryption in fog-enabled IoT environment. IEEE Transactions on Network Science and Engineering 9(6):4468–4481
3. Mukti AP, Lusiana L, Titisari D, Palanisamy S (2023) Performance analysis of twelve lead ECG based on delivery distance using bluetooth communication. J electromedical eng med inform. 5(1):46–52
4. Anitha VR, SatheeshKumar Palanisamy, Osamah Ibrahim Khalaf, Sameer Algburi, Habib Hamam (2004) Design and analysis of SRR based metamaterial loaded circular patch multiband antenna for satellite applications. ICT Express https://doi.org/10.1016/j.icte.2024.05.002
5. Mitchell R, Chen R (2019) Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. IEEE Trans Dependable Secure Comput 12(1):16–30
6. Chen Y, Kar S, Moura JM (2016) Dynamic attack detection in cyber-physical systems with side initial state information. IEEE Trans Autom Control 62(9):4618–4624
7. Satheesh Kumar P, Jeevitha, Manikandan (2021). Diagnosing COVID-19 virus in the cardiovascular system using ANN. In: Oliva, D., Hassan, S.A., Mohamed, A. (eds) Artificial Intelligence for COVID-19. Studies in Systems, Decision and Control, vol 358.Springer, Cham. https://doi.org/10.1007/978-3-030-69744-0_5
8. Palanisamy S, Thangaraju B, Khalaf OI, Alotaibi Y, Alghamdi S, Alassery F (2021) A novel approach of design and analysis of a hexagonal fractal antenna array (HFAA) for next-generation wireless communication. Energies 14(19):6204. https://doi.org/10.3390/en14196204
9. Djamaa B, Senouci MR, Bessas H, Dahmane B, Mellouk A (2021) Efficient and stateless P2P routing mechanisms for the Internet of Things. IEEE Internet Things J 8(14):11400–11414
10. Hasan MK, Islam S, Sulaiman R, Khan S, Hashim AHA, Habib S, Hassan MA (2021) Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access. 9:47731–47742
11. Liu, Jianghua et al (2003) Lightweight Authentication Scheme for Data Dissemination in Cloud-Assisted Healthcare IoT. IEEE Transactions on Computers 72:1384-1395.

12. Dogaru, Delia Ioana, Ioan Dumitrache (2015) Cyber-physical systems in healthcare networks. 2015 E-Health and Bioengineering Conference (EHB) p. 1-4.
13. Elhoseny M, Shankar K, Lakshmanaprabu SK, Maseleno A, Arunkumar N (2020) Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Comput Appl 32(15):10979–10993
14. Ukil, Arijit et al (2011) Embedded security for Internet of Things. 2011 2nd National Conference on Emerging Trends and Applications in Computer Science p. 1-6.
15. Jebril I, Dhanaraj P, Abdulsahib GM, Palanisamy SK, Prabhu T, Khalaf OI (2022) Analysis of Electrically Couple SRR EBG Structure for Sub 6 GHz Wireless Applications. Advances in Decision Sciences, Asia University, Taiwan. 26(Special):102–123
16. Palanisamy S, Thangaraju B, Khalaf OI, Alotaibi Y, Alghamdi S (2021) Design and Synthesis of Multi-Mode Bandpass Filter for Wireless Applications. Electronics 10(22):2853. https://doi.org/10.3390/electronics10222853
17. SatheeshKumar, Balakumaran T (2021) Modeling and simulation of dual layered U-slot multiband microstrip patch antenna for wireless applications. Nanoscale Reports 4(1):15 – 18. https://doi.org/10.26524/nr.4.3
18. Ghaida Muttashar Abdulsahib, Dhana Sekaran Selvaraj, A. Manikandan, SatheeshKumar Palanisamy, Mueen Uddin, Osamah Ibrahim Khalaf, Maha Abdelhaq, Raed Alsaqour, (2023) Reverse polarity optical Orthogonal frequency Division Multiplexing for High-Speed visible light communications system, Egyptian Informatics Journal 24(4):10040. ISSN 1110-8665.https://doi.org/10.1016/j.eij.2023.100407
19. Palanisamy, S., Nivethitha, T., Alhameed, M.R., Udhayakumar, A., Hussien, N.A. (2023). Urban Wastewater Treatment for High Yielding in Agriculture Through Smart Irrigation System. In: Swaroop, A., Kansal, V., Fortino, G., Hassanien, A.E. (eds) Proceedings of Fourth Doctoral Symposium on Computational Intelligence . DoSCI 2023. Lecture Notes in Networks and Systems, vol 726. Springer, Singapore. https://doi.org/10.1007/978-981-99-3716-5_52
20. Palanisamy S, Thangaraju B (2022) Design and analysis of clover leaf-shaped fractal antenna integrated with stepped impedance resonator for wireless applications. Int J Commun Syst 35(11):e5184. https://doi.org/10.1002/dac.5184
21. Kompara M, Kumari S, Hölbl M (2019) Analysis and improvement of a secure key management protocol for e-health applications. Comput Electr Eng 73:97–113
22. Palanisamy S (2022) Predictive analytics with data visualization. Journal of Ubiquitous Computing and Communication Technologies 4(2):75–96. https://doi.org/10.36548/jucct.2022.2.003
23. Qi R, Ji S, Shen J, Vijayakumar P, Kumar N (2021) Security preservation in industrial medical CPS using Chebyshev map: an AI approach. Futur Gener Comput Syst 122:52–62
24. Khari M, Garg AK, Gandomi AH, Gupta R, Patan R, Balusamy B (2019) Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems 50(1):73–80
25. Sun H, Wang X, Buyya R, Su J (2021) CloudEyes: cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices. Softw Pract Exp 47(3):421–441
26. Shivappriya SN, Palanisamy S, Mohammed Shareef A, Ali Zearah S (2023) Significance of Literacy in Minimizing Infant Mortality and Maternal Anemia in India: A State-Wise Analysis. In: Swaroop A, Kansal V, Fortino G, Hassanien AE (eds) Proceedings of Fourth Doctoral Symposium on Computational Intelligence. DoSCI 2023. Lecture Notes in Networks andSystems, vol 726. Springer, Singapore. https://doi.org/10.1007/978-981-99-3716-5_73
27. S D, Palanisamy S, Hajjej F, Khalaf OI, Abdulsahib GM, S R (2022) Discrete Fourier Transform with Denoise Model Based Least Square Wiener Channel Estimator for Channel Estimation in MIMO-OFDM. Entropy 24:1601. https://doi.org/10.3390/e24111601
28. Morii M, Tanioka H, Ohira K, Sano M, Seki Y, Matsuura K, Ueta T (2017). Research on integrated authentication using passwordless authentication method. In 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC) 1:682–685 IEEE
29. Kocabas O, Soyata T, Aktas MK (2021) Emerging security mechanisms for medical cyber physical systems. IEEE transactions on computational biology and bioinformatics 13(3):401–416
30. Kanjee MR, Liu H (2016) Authentication and key relay in medical cyber-physical systems. Security and Communication Networks 9(9):874–885
31. Palanisamy S, Rubini SS, Khalaf OI et al (2024) Multi-objective hybrid split-ring resonator and electromagnetic bandgap structure-based fractal antennas using hybrid metaheuristic framework for wireless applications. Sci Rep 14:3288. https://doi.org/10.1038/s41598-024-53443-z
32. Sam PJC, Surendar U, Ekpe UM, Saravanan M, Satheesh Kumar P (2022) A Low-Profile Compact EBG Integrated Circular Monopole Antenna for Wearable Medical Application. In: Malik PK, Lu J, Madhav BTP, Kalkhambkar G, Amit S (eds) Smart Antennas. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-76636-8_23
33. Mehmood Z, Ghani A, Chen G, Alghamdi AS (2019) Authentication and secure key management in E-health services: a robust and efficient protocol using biometrics. IEEE Access 7:113385–113397
34. Reddy VS, Rao BT (2018) A combined clustering and geometric data perturbation approach for enriching privacy preservation of healthcare data in hybrid clouds. International Journal of Intelligent Engineering and Systems 11(1):201–210
35. Caruso S, Caruso S, Pellegrino M, Skafi R, Nota A, Tecco S (2021) A knowledge-based algorithm for automatic monitoring of orthodontic treatment: the dental monitoring system. Two cases Sensors 21(5):1856
36. Suganya E, Prabhu T, Palanisamy S, Malik PK, Bilandi N (2023) A Gehlot (2023) An isolation improvement for closely spaced MIMO antenna using λ/4 distance for WLAN applications. International Journal of Antennas and Propagation 2023(4839134):13. https://doi.org/10.1155/2023/4839134
37. Abdmeziem MR, Tandjaoui D (2018) An end-to-end secure key management protocol for e-health applications. Comput Electr Eng 44:184–197
38. Shanableh T (2022) Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering. IEEE Trans. Inf. Forensics Security 7(2):455–464

39. Tian Y, Wang Z, Xiong J, Ma J (2020) A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Trans Industr Inf 16(9):6193–6202
40. Vijayakumar P, Chang V, Deborah LJ, Kshatriya BSR (2021) Key management and key distribution for secure group communication in mobile and cloud network. Futur Gener Comput Syst 84:123–125
41. Xu S, Li Y, Deng RH, Zhang Y, Luo X, Liu X (2019) Lightweight and expressive fine-grained access control for healthcare Internet-of-Things. IEEE Transactions on Cloud Computing 10(1):474–490
42. Xue X, Shanmugam R, Palanisamy S, Khalaf OI, Selvaraj D, Abdulsahib GMA (2023) Hybrid cross layer with Harris-Hawk-optimization-based efficient routing for wireless sensor networks. Symmetry 15:438. https://doi.org/10.3390/sym15020438
43. Yang Y, Liu X, Deng RH (2017) Lightweight break-glass access control system for healthcare Internet-of-Things. IEEE Trans. Ind. Informat. 14(8):3610–3617
44. Yaacoub JPA, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M (2020) Cyber-physical systems security: limitations, issues and future trends. Microprocess Microsyst 77:103201

Publisher's Note