Zero Trust Architecture for Security and Protection System in 5G Intelligent Healthcare

Wenzhong Jin
Department of Information Center
Shanghai Ninth People's Hospital and Shanghai JiaoTong University School of Medicine, China
jinwz4180@sh9hospital.org.cn

Shanjun Wu
Department of Information Center
Shanghai Ninth People's Hospital and Shanghai JiaoTong University School of Medicine, China
wushanjun@sh9hospital.org.cn

Yu Feng
Department of Information Center
Shanghai Ninth People's Hospital and Shanghai JiaoTong University School of Medicine, China
631350@sh9hospital.org.cn

Huijing Wang
Department of Information Center, Shanghai Ninth People's Hospital and Shanghai JiaoTong University School of Medicine China
631326@sh9hospital.org.cn

Chunyu Fu
Department of Information Center, Shanghai General Hospital and Shanghai JiaoTong University School of Medicine, China
cy.fu@shgh.cn

Abstract: *The fundamental attributes of the 5G network, namely its high bandwidth and concurrency, reduced latency, and ability to handle high-mobility big data platforms, render it valuable in tackling forthcoming healthcare challenges and emerging health demands like as the COVID-19 pandemic. The enforcement of the security component within a 5G-based Intelligent Healthcare System (IHS), which encompasses critical information and facilities, is more imperative and significant. In the context of deploying a healthcare system in a distributed manner, the effectiveness of passive security measures, such as information encryption and isolation, employed on traditional health platforms is insufficient to address the requirements for information and facility interchange across "cloud-edge-terminals" in the era of 5G. This study proposes a security solution for an intelligent health platform based on the Zero-Trust Model (ZTM) in the context of 5G technology. This study presents fundamental principles like the real-time monitoring of network asset security, risk evaluation of individual access requests, and access permission and decision-making through the use of a dynamic trust algorithm. The 5G IHS encompasses four primary dimensions, namely "theme" which includes people, terminals, and applications, "item" which encompasses information, platforms, and facilities, "behavior," and "environment". With the highest accuracy (98.9), precision (95.9), recall (98), and F1-score (95.5) among the several approaches, the suggested ZTM method better the others consistently. These overall numerical results for accuracy, precision, recall, and F1-score across methodologies are shown. A lower but more variable performance was shown by other approaches, including RNN, KNN, Support Vector Machine (SVM), and Dynamic Equilibrium Optimized Gated Recurrent Unit (DEO-GRU) across all measures. The proposed security system has been subjected to thorough testing and implementation at an industrial level, showcasing its ability to fulfill the criteria for dynamic shield and end-to-end safety execution of information, users, and facilities present in an Intelligent Healthcare (IH) scheme based on 5G technology.*

Keywords: *Artificial intelligence, intelligent healthcare system, sustainable development, big data, healthcare, 5G communication, information safety, security*.

Received June 11, 2024; accepted November 03, 2024
https://doi.org/10.34028/iajit/22/2/5

1. Introduction

The "intellectualization" of society is facilitated by a number of changes brought about by "Internet+" and "Intelligent+" with the development and widespread deployment of 5G technology (i.e., fifth generation of mobile communication), and this trend is also mirrored in the healthcare sector [3]. The features of 5G technology include end-to-end network slicing, a unique air interface, and a facility-oriented network model. These qualities enable 5G to effectively cater to the diverse network requirements of different applications [6, 25, 27]. Moreover, the implementation of 5G technology provides robust technical assistance in the development of Intelligent Healthcare (IH) applications. Notably, the use of 5G in the field of IH which stands as a prominent example of vertical industry applications for this advanced technology. 5G technology has demonstrated significant potential in the field of healthcare due to its capacity to facilitate the transfer and processing of large-scale health imaging data, enable ultrahigh-definition video contact, and provide real-time remote control of intelligent devices [19, 31]. Consequently, it possesses the capability to fulfil the system demands of surgical procedures performed remotely, intelligent diagnosis of medical images, interdisciplinary consultation, and several other situations related to health applications [5, 7]. The health sector is affected by issues with centralised health resources, highly populated staff, complex information schemes, and a wide range of diverse health equipment. When used in the health sector, 5G confronts several

difficulties since many health application scenarios require the integration of various health tools, programmes, and facilities.

One possible strategy for the healthcare facility model is the integration of 5G-Intelligent Healthcare System (HIS), which encompasses many technologies such as 5G, the Internet of Things (IoT), Edge Computing (EC), Fog Computing (FG), and Artificial Intelligence (AI) [36]. The advancements in 5G-IHS encompass novel healthcare facility models and products. These advancements are founded upon the fundamental ideas of remote healthcare, telemedicine, Internet and mobile healthcare. The 3rd Generation Partnership Project (3GPP) made an authorize denouncement in July 2020 on the complementary features of the R16 form of 5G. This announcement specifies that there will be further specification of the technological solution for IH in the context of 5G. Upon achieving the necessary standardisation and security protocols, it is expected that the production of various forms of 5G-IHS would see acceleration, resulting in increased accessibility to the wider populace. According to IHS Market's estimation, the market value of the health and fitness industry, facilitated by the integration of 5G technology, is projected to exceed $1 trillion [30]. There is a global emphasis on the health industry as the implementation of 5G technology accelerates its modernization efforts. Several countries have conducted studies and implemented state-of-the-art methods to promote the implementation and progress of 5G-IHS [12]. Verizon has officially announced its plans to launch a 5G core system and commercial cellular system in the United States during the latter half of 2019 [16]. China Mobile and the First Affiliated Hospital of Zhengzhou University demonstrated in October 2022 the viability of real-time diagnosis and remote ultrasound operations made possible by the 5G technology [24].

In February 2018, Vodafone and Clinic Hospital worked together to try remote treatment using 5G technology. Their goal was to create Spain's first 5G smart hospitals. In June 2019, the University Hospital of Birmingham, Together, British Telecom and West Midlands 5G (WM5G) demonstrated how 5G technology could be potentially used for remote ultrasound treatments and emergency services. A white paper on how to build up a 5G health system using elastic system slicing was released in October 2019 by the company China Cellular and Huawei, and Henan University First Associated Clinic. Using 5G cloud computing technology, China Mobile Corporation and the University of Sichuan published a plan in April 2020 to find and analyse COVID-19 protection. The aforementioned strategy employed remote CT technology utilising 5G systems as a means to mitigate and control the spread of the COVID-19 virus. The use of 5G-IHSpresents significant security and privacy concerns in comparison to traditional healthcare establishments [11]. The integration of 5G health applications has transformed conventional healthcare facilities by transitioning them from physical hospital settings to an online facility mode [1]. This transition involves the participation of many users, health equipment, information schemes, and entails the transfer of extensive volumes of health information. There will be a big effect on the quality of health centres and their day-to-day activities if there are security holes in their terminals and systems [18]. The implementation of security, safety, and risk management for 5G health applications is an ongoing research problem. Currently, there is a lack of established security standards for 5G systems and the healthcare industry's security requirements pertaining to 5G technology are also yet to be developed. The Zero-Trust paradigm, as presented in [33], is based on the premise that all individuals, events, and entities within or outside of a network and IS (information system) are considered untrustworthy unless they have undergone sufficient verification and authentication. This approach has demonstrated positive results in enhancing security measures in the context of 5G systems. The Zero-Trust concept effectively addresses the security requirements of a 5G system, which facilitates a substantial volume of sessions and interconnected devices that may provide unidentified risks. The existing Zero-Trust Models (ZTM) predominantly centre on concepts like clients, servers, and requested information within a system session. However, these models do not fully encompass all the possible security threats that arise from dynamic environments and the changing behaviours of mobile entities in 5G-IHS scenarios.

We propose a ZTM based security alertness and safety solution for 5G-based Intelligent Health (5G-IH) to accomplish this. In this study, we have made four unique contributions.

1. The prerequisites for the security and privacy of such schemes were first described, along with the security dangers that 5G systems and SH schemes face. The ZTM hypothesis is then mentioned as a viable solution, albeit it has to be developed for circumstances like 5G-IHS. The hypothesis holds that all parties are not trustworthy unless they have been authorised or confirmed to be secure.
2. A four-dimensional security model is created based on ZTM for 5G-IHSschemes [10]. The risk assessment model, trust assessment model, and access control model jointly utilise four key aspects of access, namely theme, item, environment, and behaviour. These dimensions are employed to construct an extremely fine system of session-based control of access and to continually evaluate possible dangers from various perspectives.
3. Expanding upon our four-dimensional secure strategy concept, we proposed that a layer of awareness and safety mechanism be designed for 5G-

IHS emphasizing incorporated 5G safety, Internet-of-things availability, simulated the system security, and health data relationships.

4. Finally, but also carefully evaluated the functionality and scheme performance of our recommended solution during industrial-grade operations. Our scheme offers an effective security solution for 5G-IHapplications, according to the testing findings.

The subsequent sections of this article are organised as follows: Section 2 provides an overview of the security considerations and requirements related to 5G-IHS. Section 3 introduces our ZTM the basic elements of the four-dimensional security paradigm. Finally, the design and tenets of our security vigilance and safety are covered in section 4 scheme, which utilises the proposed ZTM four-dimensional model for 5G-IHS. A production-stage testing environment is used in section 5 to highlight the assessment findings of our implemented scheme, and this work is wrapped up in section 6.

2. Related Work

With 5G-IHS, a range of health application scenarios have emerged or enhanced. For instance, 5G technology has been used to quickly build remote monitoring, remote emergency rescue, remote teaching, remote consulting, and remote surgery [17, 29]. These application scenarios pose new security difficulties while also raising patient satisfaction and hospital facilities quality. The private user information is stored in health information, the security of 5G in health care will have big effects on national, network, and information security, as well as potential impacts on patient safety in certain health application scenarios [13, 21]. Our security study is based on a set of presumptions that are described in detail below, along with a scenario for a Zero-Trust that is suggested as a shield against security threats. The attacker's objective is to get into a company's system and gain access to important information so they may either encrypt it and demand a ransom, or infiltrate it and make it available to the public. Here, it is presumed that the attacker is an outsider, not a member of the company, and that he or she is seeking to access the network by methods like email phishing. IH facilities are theme to security risks. The following aspects can be succinctly categorised as [2, 22, 23, 26]. 5G health applications create security and privacy threats by exposing patient data to theft and surveillance. Attacks on vital infrastructure are possible, and deliberate falsification of medical records might distort data and jeopardize monitoring and emergency response programs. It was important to keep in mind that the sources of the aforementioned security concerns may include both internal and external networks. In addition to the security risks to health applications stated above, 5G-IHSalso needs to address security concerns brought on by 5G technologies [4]. The 5G system may potentially encounter signalling Distributed Denial of Service or Storms (DDoS) attacks due to its extensive connection. One million connections per kilometre are supported by 5G, and traffic attacks launched by hackers utilising several terminals at once could undermine system shield. 5G technology presents issues in content identification, encryption, decoding, and traffic security because to its high bandwidth and low latency. Malware monitoring, encryption capabilities, and system security situational awareness are critical to addressing these issues [14, 20]. Traffic security assurance has become more difficult due to the transformation of communication channels brought about by edge clouds and D2D connection, which have also increased content security concerns. The need for adequate and comprehensive security safety for 5G-IHschemes is critical given the security issues with the 5G system and the susceptibility of IH. The specifications are as a cohesive governance structure, advanced security system, and versatile 5G-IHS model are needed to address diverse scenarios, access methods, and health application contexts. Uniform and scalable identity and authentication management schemes are necessary for diverse terminal types. An integrated security scheme with distributed security shield capabilities is crucial for 5G-IHS, leveraging computational capabilities to mitigate threats from Multi-access Edge Computing (MEC) and Device-to-Device (D2D) connections. The ZTM can be used to solve the aforementioned problems [8]. According to the ZTM, all system communication must first be authorised, detected, or verified as safe in order to be trusted [28]. No matter where the user accesses the information from an internal system or an external one it ensures secure access to healthcare information. By implementing least privilege regulations and carefully enforcing access control policies, the ZTM lowers harmful access and assaults [15, 34]. All system traffic is recognised, logged, and on-going user behaviour monitoring is performed. The ZTM paradigm is therefore appropriate for solving the system hazards and health application security issues that 5G-IH must deal with. The establishment of the theme, encompassing individuals and equipment, as well as the item, which pertains to information and facilities, is commonly achieved by employing established Zero-Trust security models as fundamental security dimensions [35]. However, these models are inadequate in meeting the security requirements of 5G-IH applications, particularly in terms of tracking and safeguarding against risks that arise from distributed environments and evolving behaviours. With the use of Deep Learning (DL) methods and 5G technologies, it could be able to accurately monitor diabetic patients remotely in real time. It presented the novel Dynamic Equilibrium Optimized Gated Recurrent Unit (DEO-GRU) method, which accounts for fluctuations in blood sugar, assesses intricate data patterns, and provides customized insights

for effective diabetes management [9].

3. ZTM for 5G Intelligent Healthcare

For 5G-enabled cooperation between terminals, EC nodes, cloud information-sharing tools, and apps in the field of IH to work, a setting with high cooperation, minimal latency, and capacity needs to be set up. The previously described growing shield needs of 5G-IHScannot be met by current security schemes leveraging system separation and shield-in-depth. In order to obtain fine-grained security alertness and safety capabilities, there is a necessity to overcome the physical system barrier and establish a novel network security architecture that is founded upon the utilisation of facilities and applications. Consequently, we provide a security model with four dimensions, utilising the ZTM, which centres on the aspects of people, equipment, applications, as well as the items of information, platform, and facility. This model is specifically designed for the context of a 5G-IH scheme, and is further elaborated in section 3. The expansion of the Zero-Trust notion is achieved by the utilisation of a limited number of dimensions, specifically two. The proposed model utilises dynamic access control, which involves ongoing assessment of situational security awareness, identity authentication, behaviour analysis, and fine-grained access behaviour control as outlined in section 3.4. Access controls are generated based on security and trust levels derived from various sources, including the trust assessment model discussed in section 3.3.

3.1. Four Tiers of our Proposed ZTM

Here, we outline the model's four proposed tiers for 5G-IHSscenarios.

- **Tier 1: The Theme**

Initially, the focal point of inquiry pertains to the conceptualization of the "theme" within the context of a 5G-IH information system. The entity seeking authorization to access a system or resource is commonly referred to as the subject. As depicted in Figure 1-a), the key components of a 5G-IHS encompass identity-based healthcare providers, identification-based networked healthcare and system technologies, and online healthcare applications integrated through a device's or an individual's identification. Multiple concepts might or might not prove credible over phases. As a result, more trustworthy themes (such as chief doctors) may be able to access more private resources (such as health records), whereas less trustworthy themes (such as system-connected intelligent sphygmomanometers) might not be able to access any information but only be able to upload measured information. As a result, the first aspect of 5G-IH security is the trust stage of the themes. The reliability of a person is determined by using real-time information from a variety of sources, such as names, permissions, access logs, and other relevant data. The utilisation of a greater variety of dependable information sources in the process of constructing a trust stage will result in a higher degree of accuracy in the final conclusion. The fast development of AI makes it possible to judge trust. It is possible to use AI technologies like methods for using Machine Learning (ML) and expertise systems that are closely matched to particular applications scenarios to enhance the trust assessment processes' computational effectiveness and accomplish the intended security characteristics, dependability, availability, and cost-effectiveness in the ZTM.

- **Tier 2: The Item**

Now, we describe the "item" of a 5G-IH information scheme, or the resource that an access request makes reference to. A 5G-IHSscheme includes elements including health data, IH facility functionalities, and facility interfaces, as depicted in Figure 1-b). Items are uploaded, downloaded, traded, and used by themes in an IH scenario. However, there are limitations to how you can operate on items. Sensitive information, facility functionalities, and interfaces should not be available to less reliable or irrelevant parties in order to ensure scheme security and patient privacy during health facilities. As a result, the second aspect of 5G-IH security is the item's stage of security. The security stage of an item is determined by evaluating its own assessment, environment, current threats, and other information. If a security stage were to be determined using more reliable information types, it would be more accurate.

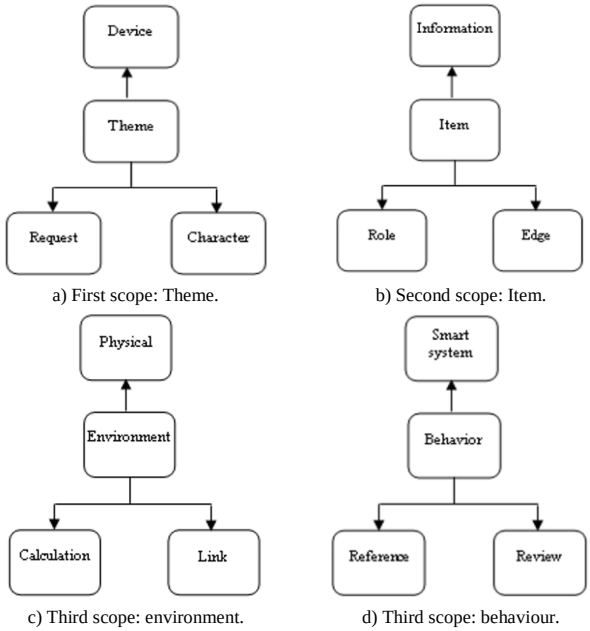
- **Tier 3: The Environment**

When talking about a 5G-IH information system, the word "environment" refers to the situational security that controls system and procedures for access to resources applications. According to Figure 1-c), within the context of a 5G-IH information scheme, the term "environment" encompasses the physical, computer, and system environments via which health and system equipment get access. The consideration of this component is often overlooked in current ZTMs, despite its significance in assessing the trustworthiness of access requests, which might be influenced by many environmental factors. One illustration of this concept is that the act of obtaining confidential health information within an exclusive treatment space entails a lower level of privacy vulnerability compared to accessing them within a communal public setting. Additionally, the provision of healthcare services through a dedicated health system offers greater security measures in comparison to using the public Internet. The security stage of the access environment, which is driven by the elements outlined earlier, constitutes the third part of IH security in the context of 5G. The level of security in the

environment is evaluated by a study of threats, which includes evaluating factors such as risk analysis, trust rating, and business connections. Additionally, risk awareness is taken into consideration, including the safety of equipment, operations, systems, applications, and terminals inside the environment.

- **Tier 4: The Behaviour**

The 'behaviour' dimension of a 5G-IH information scheme is finally specified. On the basis of recent networking behaviour, recent resource access behaviour, and history access behaviour, it comprises real-time security analysis and judgement. The field of behaviour analysis encompasses several aspects such as intelligent inference, behaviour baseline, security audit, and more within the context of a 5G-IHS, as seen in Figure 1-d). The most important factor in ensuring the trustworthiness of participating themes, items, and environments throughout a facility session is tracking dynamic and changing behaviours, as a trustworthy an entity could stop being reliable, and a safe space might stop being safe. At a moment in time adjustments could have a big impact on how securely and privately an IH facility is delivered. Hence, the fourth component of IH security in the context of 5G pertains to the real-time analysis of access behaviour. The evaluation of previous way in patterns and continuous security observation of current access patterns are employed to ascertain the security level of access behaviour.



a) First scope: Theme. b) Second scope: Item.

c) Third scope: environment. d) Third scope: behaviour.

Figure 1. The security of 5G-HIS in four scopes.

3.2. Risk Assessment Process

Our approach carries out risk assessment centred on the theme and environment dimensions. The risk judgement scheme, which will be discussed in section 3.3, uses theme trust identification and situational alertness to provide scores and thorough reports on potential dangers connected with themes and settings. These reports serve as crucial references in the trust evaluation process.

3.2.1. Approach for Risk Assessment

The access theme and environment of IH apps are the main focus of the risk assessment approach of access behaviour. The theme's assessment is driven by "controllability."

1. Whether or not networked health equipment has been fully identified, registered, and is supported by reliable hardware.
2. This inquiry pertains to the association between the identification of networked health workers and the corresponding device, the nature of authentication (local or remote), the specific technique and stage of identity authentication employed, and the extent of personnel information obtained through alternative schemes.

To change dynamic controllability, the theme's judgement must also take historical information into account. The "risk stage" generated from threat modelling is the main consideration in the assessment of the environment:

1. The operating scheme's starting safety, operating scheme baseline satisfaction, patch status, malware attack history, etc. are all examples of the software environment of an IH application.
2. The hardware environment for computing and storage, including the temperature of the main components and the presence of any additional peripherals.
3. The environment of the 5G system, including the capabilities, kind of connectivity, and accessibility point.
4. The physical settings of linked health equipment, including their location and if they are in a secure environment (such as an ambulance).

3.2.2. Identity Trust

The identification of health and system equipment is a vital technological component in the 5G-IH scheme for theme trust identification. The subject of trust identification technology, which is a vital component of the ZTM system, necessitates the continuous and unique identification of a terminal device. Consequently, it is imperative that the subsequent requirements are satisfied:

- **Accessible**: Irrespective of incidents of assaults or user misbehaviour, it is imperative to ensure that identification can always be quantified. Any situations where quantification is not feasible should be regarded as exceptional cases.
- **Trustworthy**: Identification cannot be falsified by anyone who has complete control over the terminal or by a potential attacker (such as a sniffer).

- **Unchanged**: Identification must be safeguarded against destruction and should be able to be found and repaired once it has been destroyed. When the device's operating system and core hardware haven't changed, the ID shouldn't either. It should also stay the same for the same hardware even in virtual settings like cloud computers.
- **Unique**: It is imperative that each device possess distinct identifications, and these identifications should be subject to change anytime alterations are made to the operating system or the fundamental hardware components, such as the hard disc.
- **Stable**: Even if a device temporarily fails, such as when a disc is damaged or new peripherals are added, the identification should not be changed right away, and it shouldn't be changed frequently because of a bug.

3.2.3. Contextual Consciousness

By keeping an eye on a range of clients and specialised devices, the situational alertness scheme can simultaneously determine how reliable the physical, system, and computational environments are in a 5G-IHscheme. The scheme employs security policies to decide how users with varying stages of trust should access resources. The integration of the situational alertness system with facility safety service gateways along with access management platforms are examples of access control tools forms a comprehensive ZTM scheme that facilitates equipment identity identification.

Four different alertness capabilities are available in the situational alertness scheme: alertness of fundamental security, scheme security, application compliance, and health status.

1. Basic security alertness is the capacity to identify dangers like viruses, APT assaults, and scheme flaws.
2. Scheme security alertness is the capacity to recognise threats associated with login, account, arrangements, and other factors.
3. Application compliance alertness is the capacity to identify potentially dangerous software, processes, registry keys, and other elements.
4. Health status alertness is the capacity to discern whether browsers, file activities, and desktops provide any terminal dangers.

Through a variety of physical environmental alertness sensors, the situational alertness scheme may identify the individual using a terminal, identifying physical environment dangers like UKey plugging in and unplugging, many observers, and authorised persons leaving.

3.2.4. Assessment of Risk

Risk reporting and risk scoring are both components of risk judgement. The major goal of risk scoring is to give 5G-IH equipment the ability to quickly identify trusted sources. The score can be used to determine all security access tactics for IH facilities. Risk reporting's primary goal is to offer sophisticated terminal trust identification capabilities. For fine-grained access control of IH facilities, all facilities can be evaluated based on particular criteria in the report.

3.2.5. Risk Assessing

The 5G-IH situational awareness scheme adheres to the notion of "trustworthy weighting," wherein the weights generated by the hazardous elements are aggregated and shown as percentages. This allows the strategic entity to establish appropriate security protocols for different score results. The credibility of the terminal is now defined by the situational alertness scheme using an "alertness template," which managers can modify to suit their needs. All alertness items are divided into three categories by the terminal situational alertness scheme: prospective risk, general risk, and significant risk. Table 1 displays the definitions and derivation standards for these three categories of risks.

Table 1. Risk measurement.

Risk stages	Explanation	Values
Potential risk	Less	0-15
Standard risk	Medium	15-55
High risk	High	55-100

The scoring system employed adheres to the traditional 100-point scale, wherein engaging in unsafe behaviours incurs deductions of points. As per the stipulated criteria, the administrator has the ability to establish several policy templates and metrics. The terminal's situational alertness scheme assesses and analyses the terminal's security situation from four angles: the importance of basic security measures, the effectiveness of the scheme's security measures, adherence to application compliance standards, and the overall health status of the system.

3.2.6. Risk Disclosure

The access control centre will receive a risk report from the 5G-IH situational alertness scheme based on the selected risk kinds and attributes. In order to implement a granular approach to access oversight, controlling access centre can bind particular properties and facilities.

3.3. Trust Evaluation Model

Figure 2 shows the trust assessment model, which is a key part of the ZTM that helps people learn how to evaluate trust continuously. The model is connected to the access control engine so that assessment information, such as the level of trust in themes, the level of security for resources, and the review results of the environment, is always available. This knowledge is used to decide which access control rules to choose. The

5G-IH care 4D security structure is where the trust rating method comes from. The measurement of identity confidence is based on two main ideas: IH people and IH tools. The IH personnel theme includes user identity characteristics, protection for credentials, and a study of how users act. On the other hand, the equipment topic includes device identity traits, the security state of terminals, and a study of how a scheme works. These ideas are used in the process of evaluating trust in identity. The risk judgement approach (explained in section 3.2) is used by the model to undertake situational risk determination. It aligns the trust stage of the theme with the security stage of the item. The behavioural dimension's discovery process is on-going, and it has an impact on how well the topic is trusted.

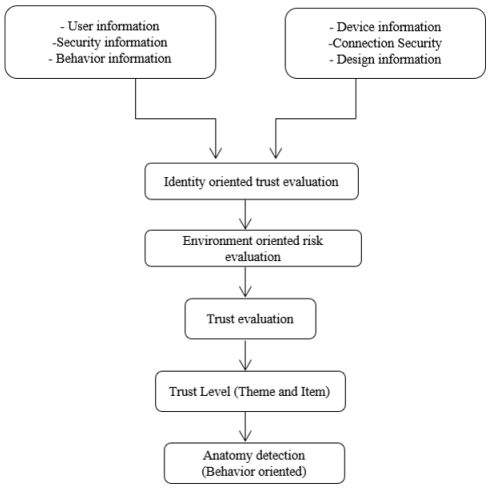


Figure 2. Proposed trust evaluation model.

The decision-making process of ZTM tactics by the access control engine is informed by the evaluation findings obtained from the trust assessment model. The model further assesses the necessity of modifying access control policies and, if deemed required, promptly terminates connections through the access agent in order to efficiently ensure resource security. During trust assessment procedures, it is envisaged that users will provide quantitative criteria to effectively handle their specific security needs. These standards may undergo enhancements via practical implementation. Consequently, it is imperative to allocate appropriate resources and establish suitable interfaces for these purposes. The ongoing dynamic evaluation of ZTM necessitates the use of many security platforms, such as early warning and monitoring systems, end-point security, threat intelligence, and security event management safety schemes. In order to facilitate ongoing and dynamic evaluation, the ZTM employs a combination of schemes that together provide information on the state of assets, regulatory obligations, security risks associated with operational environments, threat intelligence reports, and other relevant information.

3.4. Design for Access Control

When data plane with the management plane are combined into one access controls approach, creating access control rules for each request depending on information plane contact events is made easier.

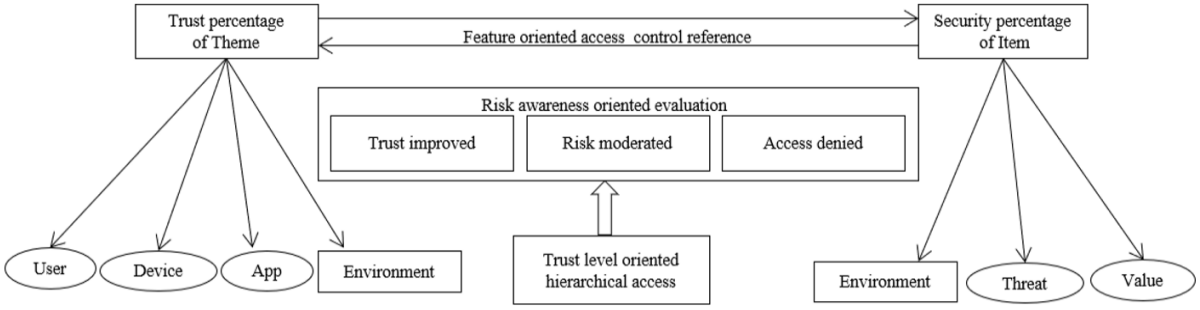


Figure 3. Proposed design of access control.

The diagram presented in Figure 3 illustrates the presence of essential trust levels and access control rights in accordance with established security laws. The proposed methodology consistently evaluates trust and adaptively adjusts access privileges based on security conditions and the principle of "minimise access control." The system employs dynamic access control limits as the sole mechanism for denying access requests from users who do not possess the requisite rights. The access control architecture utilised in our system is centred on sessions as the fundamental unit. It decides how to give rights for resource access requests by looking at the request's context, trust level, and respect to security standards. This is done by following the idea of "least privilege" and getting review results from the trust assessment model on a daily basis. The dynamic access control powers are enforced by the policy at the point where the information plane of the ZTM is. When the access agent gets a request for access, the access control engine verifies the name of the access subject and then chooses on the spot whether or not the access subject is allowed. After an access request has been authenticated, authorised, and given permission, and request is going to be directed by the access device to the restricted service over an encrypted link that shall construct. The access agent updates, suspends, or cancels the session as needed if the access control engine finds that a previously created connection needs

a policy adjustment.

4. Proposed Secure Design for Healthcare

The National Institute of Standards and Technology (NIST) first wrote about the Zero-Trust idea in its technical report SP800-207 [2]. According to using the security tenet "never trust and always verify," the model regulates how information is shared, verified, and given permission by organisations with a stake in the matter. The system is made up of an information plane that sends information about applications and a control plane that handles communication control, such as session control. The trust calculation machine and access control engine are responsible for overseeing access requests made by entities, such as clients, on the control plane, specifically for the purposes of identity authentication and authorisation. The proposed approach involves the dynamic configuration of the information plane upon the approval of an access request. Subsequently, the access agent will initiate the establishment of temporary secure connections upon receiving communication information from the relevant entities. In the context of 5G-IHS, we propose a security monitoring and protection model for ZTM. The existing model is improved in many key areas, including virtualization, information collaboration, IoT accessibility, and an integrated approach to ensuring the security of the 5G system. These enhancements are driven by the 4D security model, as discussed in section 3, and the specific requirements of IH in the context of 5G technology.

4.1. Design Outline

The security vigilance and safety model are divided into three separate logical domains, as shown in Figure 4 the information domain, the ZTM dynamic access control domain, and the user domain.

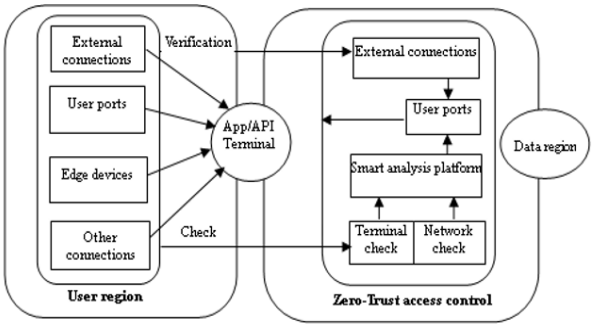


Figure 4. Model of ZTM Security.

4.1.1. User Section

The user section serves the purpose of enabling the connection of IoT devices from the edge, allowing for the invocation of interfaces from other platforms, providing access to facilities through user terminals, and ensuring secure terminal contact for operational and maintenance purposes. The user area functions indicated above all initiate a Transport Layer Security (TLS) connection with the access agent.

4.1.2. Control Section of ZTM Access

Three essential parts-the access control machine, the trust assessment machine, and the access representative-are present in the ZTM access control area that is created using the 4D security model.

- *Trust evaluation machine*: within the context of our 4D ZTM security architecture, the ongoing trust evaluation procedure is facilitated by the trust evaluation machine, which encompasses the risk evaluation model. The system operates in conjunction with the access control machine, providing ongoing evaluations of the reliability of themes, the security of their resources, the system environment, and other aspects that serve as the foundation for the development of access control techniques.
- *Access control machine*: the trust evaluation engine consistently transmits assessment findings to the access control machine, which enforces the access control machine inside our 4D model. In the ultimate evaluation, it determines whether or not to provide approval to a plan. The allocation of resources is assessed on a per-request basis and granted in accordance with the principles of least privilege. This process takes into consideration dynamic policies pertaining to request content, stages of trust, and safety regulations.
- *Access representative*: the access manager, situated within the information plane, is responsible for executing the various operations associated with unit of dynamic access control. The access manager performs identity verification upon receiving access requests in order to expedite the decision-making process pertaining to access credentials. The agent establishes secure routes for authorised persons with appropriate rights to access secured resources. When the access control engine makes modifications to the pertinent policies, the access manager subsequently alters, dismisses, or discontinues a linking or connection.

4.1.3. Information Section

The components comprising the information segment is included in the operating and storage environment for access objectives, the cloud environment, and the edge. Access to the information section will be granted after the assessment and authorization process is successfully completed inside the ZTM dynamic access control zone.

4.2. Execution of Security in Virtualized Schemes

The utilisation of virtualization is prevalent in the context of 5G-IH applications. Open-source technology

is advantageous for healthcare applications that utilise cloud and EC due to its dynamic and progressive nature. One aspect to consider is that 5G systems make use of Network Function Virtualization (NFV) technology to implement system slicing, while also relying on virtualized IT infrastructure. This Security concerns are increased and new attack surfaces are introduced when virtualization is integrated into 5G communication systems. Furthermore, the usage of publicly available open-source code and frameworks, presents significant security risks as attackers may exploit these resources. Potential results may encompass instances of information breaches resulting from vulnerabilities in containers, as well as heightened attacks on container infrastructures. The security measures and defensive strategy used for 5G-IH involve the utilisation of virtualized ZTM access control. The system utilises cloud computing technologies to provide communication and information access only for dynamically approved activities, while maintaining continuous monitoring and control.

4.3. Execution of Security in Information Relationship

The proliferation of IH applications has significantly increased the volume of internal information flow, while traditional security equipment remains predominantly designed for external facility models. Hence, the use of obsolete security methods inside the internal infrastructure of the information centre gives rise to a range of concerns, including difficulties in implementation, increased computing burden, and inflexible policy management. Using micro-segmentation technologies, the suggested model for 5G-IHS security, alertness, and safety establishes system environment isolation, end-to-end segmentation, and cross-domain segmentation. These segmentation techniques are dynamically adjusted in real-time to effectively respond to events and fluctuations in system conditions. Furthermore, for the sake of ensuring logical coherence and uniformity, this research does not go into the examination of other pertinent security technologies, such as information encryption, that have been incorporated into our proposed system.

4.4. Execution of Security for IoT Access

The management of a substantial array of IoT devices with diverse types and connecting protocols has become imperative for an IH platform, owing to the expansion of IH facilities. Hence, it is important to maintain constant management of access to the aforementioned servers and devices in order to achieve optimal efficiency and security in operations. In the event that appropriate measures are not implemented, proficient adversaries have the potential to exploit vulnerabilities present in interconnected devices, therefore launching attacks on the platform from an inside standpoint. This heightened risk arises due to the substantial quantity of interconnected IoT devices and their inherent deficiencies in terms of security capabilities. The 5G-IHSsecurity system used in our design incorporates a ZTM for secure access to IoT devices. The system accomplishes authentication of identities and workstation access control by leveraging EC. It enables access to allowed IoT devices in a dynamic manner, ensuring reliability. Furthermore, it monitors the real-time activity of these devices and promptly detects and manages any fraudulent or unlawful connections.

4.5. Secure 5G Network Integration

The integration of many apps onto a unified network is facilitated by the implementation of 5G technology. This technology enables network segmentation and application support through the use of network slicing and EC techniques. Nevertheless, the use of diverse security measures is essential. In addition to the safety holes in 3G, 2G, and 4G networks, there are also 5G networks' numerous features, including the terminal, edge, and might, present additional risks. Our ZTM solution is employed to handle the security concerns pertaining to the IT infrastructure, the 5G-IH applications, and the mobile communication networks. A combined 5G network alert system and an ad hoc approach are used to create the security model. This architecture includes automated access control policy creation, granular user access control methods, and unified 5G identity management solutions. The modification is implemented while maintaining the original architecture of the 5G core network.

5. Performance Evaluation

We established a testing environment to evaluate the functionality of each element and the overall performance of the 5G-IH security alertness and safety scheme employing ZTM. Functionality testing and scheme performance testing made up the two portions of the exam. To determine if the overall scheme complies with the predicted functional criteria, the functionality examination covered the functional elements at all stages. After scheme integration, the scheme performance examination showed that the scheme could deliver facilities, including dependability, safety, and maintainability.

5.1. Testing Platform

We built up an examination environment in accordance with the verification requirements, as depicted in Figure 5. All of the environment's hardware, including the servers, client terminals, and network capacity, are of the production-grade variety and are suitable for use in actual operations.

The n environment represents the implementation of the structural components of our system, namely the

user area, access agent, ZTM dynamic access control area, and information area (as seen in Figure 4). The devices often found in the user area are laptops and cell phones that have direct connections to the platform of a trusted agent. The attainment of situational awareness is facilitated via the implementation and incorporation of applications such as Jira, Wiki, and Traffic Probe on the trust agent platform.

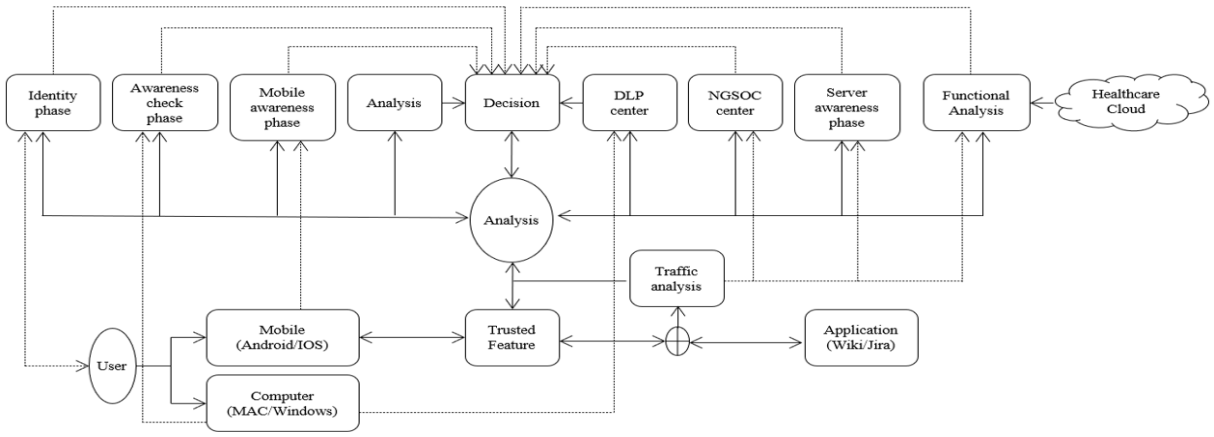


Figure 5. Testing platform of proposed model.

5.2. Functionality Assessment

The functional elements of the entire scheme were covered by the functional examinations. The outcomes of important elements are as follows.

5.2.1. Segment for User Access Behaviour Examination

Table 2 presents detailed information on the outcomes of tests and the many scenarios examined in relation to the study of user access behaviour. Unit exams are offered for the primary components of the user access behaviour analysis module, encompassing log reception, peer network analysis, access behaviour analysis, Pareto testing, and unauthorized access research. The database has been effectively loaded with all scheme logs in accordance with the unit examination for log reception. Peer group analysis is performed in order to ascertain that the necessary access control exceptions are activated in response to anomalous actions related to group behaviour. Unauthorised access refers to the process of verifying whether appropriate access control exceptions are implemented for specific behaviours. Pareto analysis reveals that the implementation of essential access control mechanisms is crucial in preventing individual-based illegal conduct. The user access behaviour assessments assess the scheme's ability to effectively manage unusual user access patterns and produce precise trust credits.

Table 2. Behaviour analysis of user access.

Cases	Outcomes	Results	Error
1	Logs are successfully stored in database	Success	No
2	Trigger exception for user access	Success	No
3	Trigger exceptions for user requests	Success	No
4	Trigger exceptions for user authentication	Success	No
5	Individual exceptions authentication	Success	No
6	User authorized exceptions	Success	No
7	Access time analysis	Success	No
8	User abnormal behaviour calculation	Success	No
9	Credit calculation	Success	No

5.2.2. Segment for Equipment Risk Examination

Table 3 lists the specific examination scenarios and outcomes for the equipment risk judgement element. We ran unit examinations for "functionality" and "exception" on this element. Functionality examinations confirm that security arrangements have been implemented appropriately, and the examination for exceptions demonstrates how the scheme operates in an unexpected situation. It is evident that the results of the unit examinations for functionality and exception handling are accurate and provide the appropriate status and error codes.

Table 3. Risk evaluation analysis.

Cases	Outcomes	Results	Results	Error
1	In compliance with the Tess template, the policy check item "configuration of software blacklist" was successfully confirmed.	Verified, item is correct accurate	Success	No
2	According to the Tess model, the rule check point "configuring software white list" was suitably checked.	Verified, item is correct accurate	Success	No
3	According to the Tess template, the rule check item "exposure upgrade state" has been successfully identified.	Verified, item is correct accurate	Success	No
4	According to the Tess model, the policy check point "Audit log size settings" is duly checked.	Verified, item is correct accurate	Success	No
5	When receiving address, no exception is raised if the Tess template is not configured.	There is no exception made	Success	No
6	In instances when the Tess template address cannot be found, an exception is not thrown.	There is no exception made	Success	No

5.2.3. Trust Measurement Segment

Table 4 displays specifics of examination results and examination cases for the trust assessment element. Unit examinations were run for this element's functionalities, including the computation of the trust model, the computation of the trust baseline, and the execution of

the trust push and resolution strategies. The examinations for computation of the trust model confirm the accuracy of the model's actions, the trust push and resolution tests strategies verify the precision of strategy arrangements, and the examinations for trust baseline calculation verify the viability of configured security baselines. All examinations came back with the expected outcomes.

Table 4. Trust evaluation segment.

No.	Cases	Highlights	Outcomes	Error
1	Customizable baseline trust stages come in five categories.	The stages are successfully customised.	Success	No
2	For each stage's baseline arrangement, a diagram is produced.	The diagram is successfully produced.	Success	No
3	Each trust calculation methodology is open to changes.	The enable/disable status changes are effective.	Success	No
4	It becomes operational to enable and disable each trust computing paradigm.	The enabled trust models continue to calculate while the disabled trust models cease.	Success	No
5	Within the allotted time, the trust resolution technique is effective.	Within the allotted period, strategies are successful.	Success	No
6	It is possible to add, remove, modify, and query trust push policies.	Successful addition, deletion, modification, and querying of policies.	Success	No
7	The push strategy can transmit a specific object's trust change information to a particular receiver.	The associated trust change is successfully pushed.	Success	No

5.2.4. Decision Segment

The details of examination scenarios and outcomes are shown in Table 5 for the risk decision element. The examinations for the element attest to the precision of the risk generation, risk handling, and establishment of relevant policies. Each outcome is correct since unit testing is used to put its features to the examination.

Table 5. Analysis of risk decision element.

No.	Cases	Highlights	Outcomes	Error
1	With accuracy, each risk derivation rule is inserted and matched.	Correctly inserted and matched rules.	Success	No
2	Rules for eliciting risks under "&&" are inserted and matched correctly.	Correctly inserted and matched rules.	Success	No
3	Delete-able risk derivation rules.	Rules have been successfully deleted.	Success	No
4	The risk management strategy's daily hit numbers are accurate.	Statistics are reliable.	Success	No
5	The risk management strategy's historical hit numbers are accurate.	Statistics are reliable.	Success	No
6	Changes to the third-party address take effect immediately.	Changes take effect in the following period.	Success	No
7	Changes to the "action" in the policy take effect right away.	Changes are effective right away.	Success	No
8	Multiple policies are in effect after matching.	Several rules go into effect.	Success	No

5.3. Comparative Outcomes

The proposed method ZTM of the study compared with other existing methods such as recurrent neural network (RNN) [9], k-Nearest Neighbours (KNN) [9], Support Vector Machine (SVM) [9], and DEO-GRU [9]. The suggested ZTM approach showed the best accuracy, proving to be more effective than the other approaches [32].

5.4. Accuracy

The capacity of the system to accurately recognize and react to threats or illegal access is referred to as accuracy in 5G IH. It assesses how well the system minimizes false positive and negatives to uphold a safe and dependable healthcare environment, safeguards private information, and identifies any security breaches. Table 6 and Figure 6 represent the outcomes of accuracy.

Table 6. Outcomes of accuracy.

Methods	Accuracy
RNN	90
KNN	93
SVM	83.9
DEO-GRU	95.2
ZTM (Proposed)	98.9

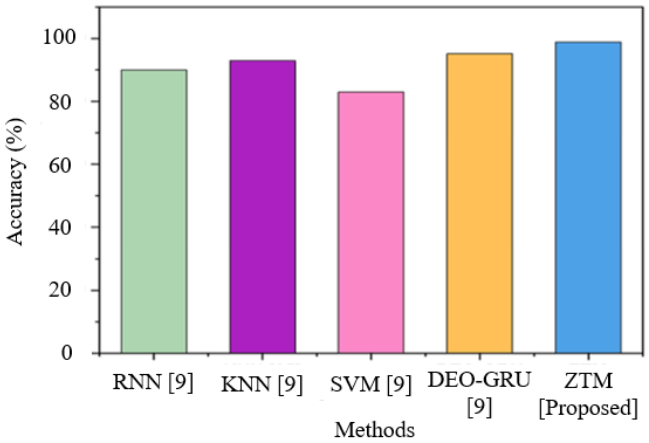


Figure 6. Results of accuracy.

The RNN's accuracy was 90.0, and the KNN's was slightly better at 93.0. At 83.9, the SVM method's accuracy was the lowest. DEO-GRU displayed a 95.2 percent accuracy improvement. When compared to the other approaches, the suggested ZTM method performed better, with the greatest accuracy of 98.9.

5.5. Precision

Precision describes the system's capacity to precisely detect and neutralize security threats, protecting privacy and data integrity in the context of a 5G safety and defence system IH's. It entails reducing the number of false positives and negatives in threat detection, which improves the security and efficacy of the hospital network's defences. Table 7 and Figure 7 represent the outcomes of precision.

Table 7. Outcomes of precision.

Methods	Precision
RNN	88
KNN	92
SVM	83.7
DEO-GRU	93
ZTM (Proposed)	95.9

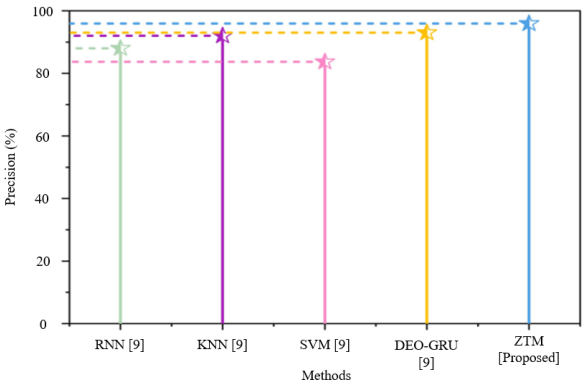


Figure 7. Results of precision.

Following a comparative analysis of several security and protection system methods, the following precision results were obtained: 88% for the RNN, 92% for the KNN method, 83.7% for the SVM and 93% for the DEO-GRU. The suggested ZTM approach outperformed the precision of 95.9% better than the existing methods.

5.6. Recall

The term recall in 5G IH security and protection system's capacity to recognize and get pertinent security measures and protocols in to handle and mitigate risks. Using sophisticated encryption, authentication, and real-time monitoring inside the 5G network, the goal entails ensuring data privacy, stopping unwanted access, and shielding medical information from intrusions. Table 8 and Figure 8 illustrate the outcomes of recall.

Table 8. Outcomes of recall.

Methods	Recall
RNN	95.2
KNN	93.6
SVM	70
DEO-GRU	97.8
ZTM (Proposed)	98

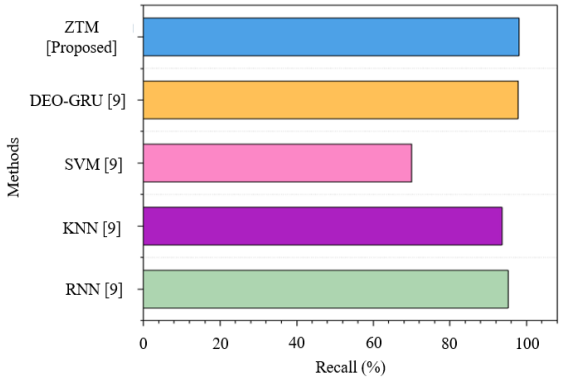


Figure 8. Results of recall.

The recall ratings for various techniques in the security and protection system evaluation are as follows: The results for RNN were 95.2%, KNN was 93.6%, SVM was 70%, DEO-GRU was 97.8%, and the suggested ZTM technique was 98%. This suggests that the ZTM approach outperformed the others in detecting pertinent security concerns, as seen by its greatest recall.

5.7. F1-Score

By balancing false positives and false negatives, the F1-score calculates the harmonic mean of precision and recall to access the accuracy of a model. With the framework of 5G IH's security and protection systems, the F1-score assesses how well the system minimizes false alarms and detects and prevents security threats, ensuring strong patient data security and system integrity. Table 9 and Figure 9 depict the outcomes of F1-score.

Table 9. Outcomes of F1-score.

Methods	F1-score
RNN	89
KNN	92
SVM	83.9
DEO-GRU	95
ZTM (Proposed)	95.5

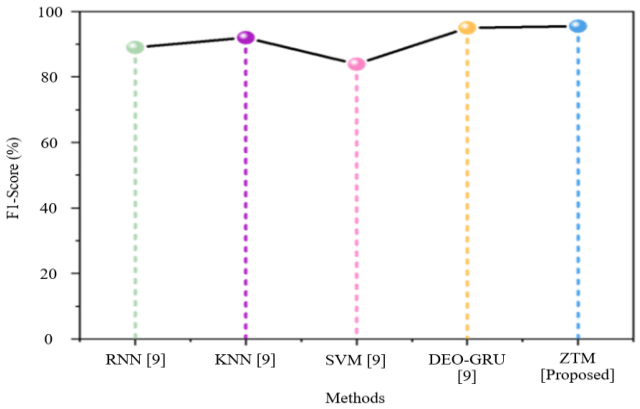


Figure 9. Results of F1-score.

The following are the numerical results for the F1-scores using various methods: The F1-scores for the RNN, KNN, SVM, DEO-GRU, and the suggested ZTM approach were as follows: 89, 92, 83.9, 95, and 95.5, respectively.

6. Conclusions and Discussions

This study introduces a security awareness and safety solution for IH in the context of 5G technology, utilising the ZTM. This study aims to present a theoretical model for IH in the context of 5G technology, incorporating four dimensions: theme, item, environment, and behaviour. The motivation for this design stemmed from the advancement of 5G-HIS and the subsequent concerns over security. In this study, we conducted an examination of the security measures implemented for comprehensive 5G network security, IoT access, data

cooperation, and virtual network architecture. The goal of this analysis was to provide the foundation for our security surveillance and safety model, as well as to address the security requirements of 5G-IH applications. In the realm of 5G-IHS, it is acknowledged that there exist several issues pertaining to our zero-trust security measures and safeguards. These challenges encompass technological implementation as well as the need to enhance public consciousness. Nevertheless, the evaluation of a security solution's maturity utilising ZTM lacks a universally acknowledged methodology. Additionally, the 5G-HIS industry still has challenges with compatibility with existing security models. Consequently, there is a need for further endeavours to provide a comprehensive security awareness and safeguarding model for the deployment of 5G-IHS. The implementation of our strategy has been executed and subjected to thorough performance and functional testing. Our team is now engaged in extensive research and development of security vigilance and safety solutions utilising ZTM. The suggested ZTM technique consistently beat others with the greatest accuracy (98.9), precision (95.9), recall (98), and F1-score (95.5) among the various ways, according to the total numerical outcomes for accuracy, precision, recall, and F1-score. Other methods, such as RNN, KNN, SVM, and DEO-GRU, performed lower overall, albeit their performance varied across all criteria. The enhancements are being made based on input received from practical implementations, as well as the frameworks, models, and strategy outlined in this article.

Authors' Contributions

Wenzhong Jin: Conceptualization of experimental ideas, investigation, visualization of experimental results, original draft writing. Shanjun Wu: Data organization, review and revision of draft, formal analysis. Yu Feng: Validation, experimental supervision and guidance. Huijing Wang: Software, experimental verification. Chunyu Fu: Methodology, review and revision of the draft.

References

[1] Al-Turjman F., Ever E., and Zahmatkesh H., "Small Cells in the Forthcoming 5G/IoT: Traffic Modelling and Deployment Overview," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 28-65, 2019. DOI:10.1109/COMST.2018.2864779

[2] Batista E., Moncusi M., Lopez-Aguilar P., Martinez-Balleste A., and Solanas A., "Sensors for Context-Aware Smart Healthcare: A Security Perspective," *Sensors*, vol. 21, no. 20, pp. 1-60, 202. https://doi.org/10.3390/s21206886

[3] Cavalcante R., Stanczak S., Schubert M., Eisenblaetter A., and Tuerke U., "Toward Energy-Efficient 5G Wireless Communications Technologies: Tools for Decoupling the Scaling of Networks from the Growth of Operating Power," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 24-34, 2014. DOI:10.1109/MSP.2014.2335093

[4] Chavez-Santiago R., Szydełko M., Kliks A., Foukalas F., Haddad Y., Nolan K., Masonta M., and Balasingham I., "5G: The Convergence of Wireless Communications," *Wireless Personal Communications*, vol. 83, no. 3, pp. 1617-1642, 2015. https://pubmed.ncbi.nlm.nih.gov/27076701/

[5] Chen M., Ma Y., Song J., Lai C., and Hu B., "Smart Clothing: Connecting Human with Clouds and Big Data for Sustainable Health Monitoring," *Mobile Networks and Applications*, vol. 21, pp. 825-845, 2016. https://doi.org/10.1007/s11036-016-0745-1

[6] Chien H., Lin Y., Lai C., and Wang C., "End-to-End Slicing as a Service with Computing and Communication Resource Allocation for Multi-Tenant 5G Systems," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 104-112, 2019. DOI:10.1109/MWC.2019.1800466

[7] Ding A. and Janssen M., "Opportunities for Applications Using 5G Networks: Requirements, Challenges, and Outlook," *in Proceedings of the 7th International Conference on Telecommunications and Remote Sensing*, Barcelona, pp. 27-34, 2018. https://doi.org/10.1145/3278161.3278166

[8] Flanigan J., "Zero Trust Network Model," *Tufts Medford University*, pp. 1-7, 2018. https://www.cs.tufts.edu/comp/116/archive/fall2018/jflanigan.pdf

[9] Kapse V., Joshi M., Karthikeyan M., and Choudhary D., "A 5G-Enabled Intelligent Healthcare Sector with Deep Learning Assistance," *Multidisciplinary Science Journal*, vol. 6, pp. 1-10, 2024. DOI:10.31893/multiscience.2024ss0306

[10] Kerman A., Borchert O., Rose S., and Tan A., "Implementing a Zero Trust Architecture," *Draft, National Institute of Standards and Technology*, pp. 1-20, 2020. https://www.nccoe.nist.gov/sites/default/files/legacy-files/zt-arch-project-description-draft.pdf

[11] Khan R., Kumar P., Jayakody D., and Liyanage M., "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 196-248 2019. DOI:10.1109/COMST.2019.2933899

[12] Khanh Q., Hoai N., Manh L., Le A., and Jeon G., "Wireless Communication Technologies for IoT

in 5G: Vision, Applications, and Challenges," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-12, 2022. https://doi.org/10.1155/2022/3229294

[13] Le-Dang Q. and Le-Ngoc T., *Handbook of Smart Cities: Software Services and Cyber Infrastructure*, Springer, 2018. https://link.springer.com/chapter/10.1007/978-3-319-97271-8_1

[14] Lo N. and Tsai H., "A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1-10, 2009. DOI:10.1155/2009/125348

[15] Martimiano T., Martina J., Olembo M., and Carlos M., "Modelling User Devices in Security Ceremonies," *in Proceedings of the Workshop on Socio-Technical Aspects in Security and Trust*, Vienna, pp. 16-23, 2014. DOI:10.1109/STAST.2014.11

[16] Medin M. and Louie G., "The 5G Ecosystem: Risks and Opportunities for DoD," *Defense Innovation Board Washington DC United States*, pp. 1-33, 2019. https://apps.dtic.mil/sti/citations/AD1074509

[17] Ng C. and Reaz M., "Evolution of a Capacitive Electromyography Contactless Biosensor: Design and Modelling Techniques," *Measurement*, vol. 145, pp. 460-471, 2019. https://doi.org/10.1016/j.measurement.2019.05.031

[18] Nguyen D., Pathirana P., Ding M., and Seneviratne A., "Blockchain for 5G and beyond Networks: A State of the Art Survey," *Journal of Network and Computer Applications*, vol. 166, pp. 102693, 2020. https://www.sciencedirect.com/science/article/abs/pii/S1084804520301673

[19] Ordonez-Lucena J., Ameigeiras P., Lopez D., Ramos-Munoz J., Lorca J., and Folgueira J., "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80-87, 2017. DOI:10.1109/MCOM.2017.1600935

[20] Park J., Rathore S., Singh S., Salim M., Azzaoui A., Kim T., and Park J., "A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions," *Human-Centric Computing and Information Sciences*, vol. 11, no. 3, pp. 1-22, 2021. https://hcisj.com/data/file/article/202101282/hcis.pdf

[21] Penttinen J., *5G Explained: Security and Deployment of Advanced Mobile Communications*, John Wiley and Sons, 2019. https://ieeexplore.ieee.org/book/8788358

[22] Pussewalage H. and Oleshchuk V., "Privacy Preserving Mechanisms for Enforcing Security and Privacy Requirements in E-Health Solutions," *International Journal of Information Management*, vol. 36, no. 6, pp. 1161-1173, 2016. https://doi.org/10.1016/j.ijinfomgt.2016.07.006

[23] Qian H., Li J., Zhang Y., and Han J., "Privacy-Preserving Personal Health Record Using Multi-Authority Attribute-Based Encryption with Revocation," *International Journal of Information Security*, vol. 14, pp. 487-497, 2015. https://link.springer.com/article/10.1007/s10207-014-0270-9

[24] Qureshi H., Manalastas M., Ijaz A., Imran A., Liu Y., and Al Kalaa M., "Communication Requirements in 5G-Enabled Healthcare Applications: Review and Considerations," *Healthcare*, vol. 10, no. 2, pp. 293, 2022. https://pubmed.ncbi.nlm.nih.gov/35206907/

[25] Rost P., Mannweiler C., Michalopoulos D., Sartori C., Sciancalepore V., Sastry N., and Bakker H., "Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72-79, 2017. DOI:10.1109/MCOM.2017.1600920

[26] Sahi M., Abbas H., Saleem K., Yang X., Derhab A., Orgun M., Iqbal W., Rashid I., and Yaseen A., "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," *IEEE Access*, vol. 6, pp. 464-478, 2017. DOI:10.1109/ACCESS.2017.2767561

[27] Sattar D. and Matrawy A., "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," *in Proceedings of the IEEE Conference on Communications and Network Security*, Washington (DC), pp. 82-90, 2019. DOI:10.1109/CNS.2019.8802852

[28] Schanzenbach M., Kilian T., Schutte J., and Banse C., "Zklaims: Privacy-Preserving Attribute-based Credentials Using Non-Interactive Zero-Knowledge Techniques," *arXiv Preprint*, vol. arXiv:1907.09579, pp. 1-8, 2019. https://arxiv.org/abs/1907.09579

[29] Suciu G., Suciu V., Martian A., Craciunescu R., Vulpe A., Marcu I., Halunga S., and Fratu O., "Big Data, Internet of Things and Cloud Convergence-An Architecture for Secure e-Health Applications," *Journal of Medical Systems*, vol. 39, pp. 1-8, 2015. https://link.springer.com/article/10.1007/s10916-015-0327-y

[30] Teece D., "5G Mobile: Impact on the Health Care Sector," *Working Paper*, pp. 1-17, 2017. https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/brg_qualcomm_5g_impact_healthcare_paper_final_oct26.pdf

[31] Vergutz A., Prates N., Schwengber B., Santos A., and Nogueira M., "An Architecture for the Performance Management of Smart Healthcare

Applications," *Sensors*, vol. 20, no. 19, pp. 1-18, 2020. https://doi.org/10.3390/s20195566

[32] Vijayaraj N. and Arunagiri S., "Intensification and Interpretation of Performance in 5G Adopting Millimeter Wave: A Survey and Future Research Direction," *The International Arab Journal of Information Technology*, vol. 20, no. 4, pp. 600-608, 2023. DOI: 10.34028/IAJIT/20/4/6

[33] Wang Y., Hori Y., and Sakurai K., "On Securing Open Networks through Trust and Reputation-Architecture, Challenges and Solutions," *in Proceedings of the 1st Joint Workshop on Information Security*, Seoul, pp. 1-17, 2006. https://scholar.google.co.jp/citations?user=KdVX5OIAAAAJ&hl=en

[34] Xiaorong F., Shizhun J., and Songtao M., "Research on Industrial Big Data Information Security Risks," *in Proceedings of the IEEE 3rd International Conference on Big Data Analysis*, Shanghai, pp. 19-23, 2018. DOI:10.1109/ICBDA.2018.8367644

[35] Yu B., Wright J., Nepal S., Zhu L., Liu J., and Ranjan R., "IoTChain: Establishing Trust in the Internet of Things Ecosystem Using Blockchain," *IEEE Cloud Computing*, vol. 5, no. 4, pp. 12-23, 2018. DOI:10.1109/MCC.2018.043221010

[36] Zheng J., Wang Y., Zhang J., Guo W., Yang X., Luo L., Jiao W., Hu X., Yu Z., Wang C., Zhu L., Yang Z., Zhang M., Xie F., Jia Y., Li B., Li Z., Dong Q., and Niu H., "5G Ultra-Remote Robot-Assisted Laparoscopic Surgery in China," *Surgical Endoscopy*, vol. 34, no. 11, pp. 5172-5180, 2020. https://pubmed.ncbi.nlm.nih.gov/32700149/

Wenzhong Jin born in January, 1982, is the CIO of Shanghai Ninth People's Hospital Affiliated to Shanghai Jiao Tong University School of Medicine, Shanghai, China. He received a Master of Stomatology in Stomatology from Shanghai JiaoTong University School of Medicine.

Shanjun Wu born in June, 1986, is a Network and Information Security Engineer at Shanghai Ninth People's Hospital Affiliated to Shanghai JiaoTong University School of Medicine, Shanghai, China. He received a Bachelor of Engineering in Stomatology from the University of Shanghai for Science and Technology.

Yu Feng born in July 1980, is an Intermediate Engineer at Shanghai Ninth People's Hospital Affiliated to Shanghai Jiao Tong University School of Medicine, Shanghai, China. He received a Bachelor of Computer Science and Technology from Shanghai Jiao Tong University.

Huijing Wang born in February 1982, is a Clerk at Shanghai Ninth People's Hospital Affiliated to Shanghai Jiaotong University School of Medicine, Shanghai, China. He received a Master of Computer Science and Technology from ShanghaiTech University.

Chunyu Fu born in April 1981, is the Director of the IT Department at Shanghai General Hospital, Shanghai, China. He received a Master of Public Administration from China Southwest University.