

# GTCS-Vagus Nerve Stimulator Automation Using Private IoT-Blockchain Smartcontract

G. Karthikeyan\* and G. Kousalya

Coimbatore Institute of Technology, Coimbatore, India

\*Corresponding Author: G. Karthikeyan. Email: karthikeyan.g@cit.edu.in

Received: 23 December 2021; Accepted: 18 February 2022

**Abstract:** Generalized Tonic Clonic Seizure (GTCS) is a form of epileptic seizure in which a patient loses control over their entire body, ultimately leading to loss of consciousness. The Vagus Nerve Stimulator (VNS) is a tool/method for treating epileptic episodes that sends counter-electrical stimulations to the Vagus Nerve in order to mitigate epileptic signals from the brain. The machine is a stand-alone device that depends on human decision-making. The proposed framework uses an IoT and Blockchain oversight mechanism to augment the device's transparency. The system counteracts against false-activation by monitoring the patient's vitals through a smart watch and allows only legitimate use. The nominal operating threshold is determined by preprocessing inferences that include an 18-year-old GTCS epileptic patient and a data set of 281 non-GTCS epileptic patients. The proposed system functions as a dual control lock where the IoT system and the manually activation system work in tandem to activate the device. Based on the values sensed by the IoT device, the deployed system is able to make decisions and regulate the use of the VNS. The IoT-Blockchain framework is able to fully eradicate false activation by increasing accuracy and transparency, ensuring the device is used correctly and safely.

**Keywords:** IoT; GTCS; vagus nerve stimulator; blockchain; smart contract

## 1 Introduction

Epilepsy or Epileptic seizure is an episodic event of loss of consciousness (LOC) with tonic or clonic movements of the limbs. The patient may also have seizures in one part of the body with or without LOC. There is another type of seizure wherein the patient is unaware of the surroundings and may undertake bizarre movements like clapping, walking, and tapping of feet, licking of lips etc. The patients suffering from epilepsy require medication. Of the total GTCS epileptic patients, a meagre amount (10%–20%) of patient shave drug resistant seizures. & require surgery. Some of them benefit with Vagus Nerve Stimulation (VNS). The paper focuses on GTCS Epilepsy where the patient is rendered completely incapable of lucid movements until the epileptic episode subsides and their vitals return to baseline [1] established through clinical observations that a patient while going through a full body clonic seizure will have a 30% (approx.) increase in blood pressure (BP) and heart rate (HR) when compared to the patients'



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

nominal readings [2,3]. When the episode subsides, the patient shows a decrease in blood pressure and heart rate then gradually attains nominal values [4]. This phenomenon of rise and fall in blood pressure (unique to the patients' vitals) is digitally quantified to binary values/limits that can serve to substantiate the activation of the VNS device. The proposed algorithm utilizes the nominal Mean Arterial BP (MAP), Systolic BP (SBP), Diastolic BP (DBP) and HR as threshold within which the device remains in standby mode. On slipping over the threshold, the proposed device follows the activation protocol as described by the proposed system.

The vitals of an 18-year-old myoclonic epilepsy patient with no cardiovascular, respiratory or endocrine co-morbidities are included in the article to extract inferences [5]. Their findings corroborate the observations of a  $\pm 30\%$  increase in blood pressure and heart rate. The argument is seconded by another research by K. G. Hampel consisting of 37 patients who suffered from focal seizures [6]. The data documented a grand total of 45 instances of seizure episodes. The results show a 33%–35% increase in blood pressure and a 44%–53% increase in heart rate when compared to the patient's individual baseline value.

Nass [7] also corroborates the rise in BP and heart rate by 20%–30% and returning to baseline after 10 s. These observations of increase were observed in focal epileptic seizures where a patient loses consciousness during the episode of a seizure.

Zijlmans [8] observes the variations in heart rate during the onset of focal epilepsy. The work documents 281 seizures from 81 patients which observe a 10-beat variation in the heart rate of patients suffering from seizures. This variation is especially pronounced during the onset of a seizure.

VNS is an embedded device that is implanted into the patient to counteract the signals from the brain causing seizures in the body. The device sends a counter electrical pulse that neutralizes the epileptic signals from the brain or to a certain extent minimizes the seizure signals making the episode at least bearable. VNS is a standalone battery-operated device that is activated externally by a magnetic wand either by the patient who may sense an oncoming seizure or by a caregiver. But the device does not account for out-of-context activation wherein the device is activated during baseline conditions [9]. Out-of-context activation must be eliminated to keep the system safe [10]. The paper presents an IoT-Blockchain based VNS device that has an oversight by smart devices and accountability through Blockchain reports.

The paper is divided into three sections: i) State-of-Art ii) the proposed IoT-Blockchain based system iii) Enhancement of IoT-VNS through Blockchain smart contract and iv) Results and discussions.

## 2 Related Work

The state-of-art in this paper involves the study of the Vagus Nerve Stimulation device's experimental inferences through analysis of cardiac output, respiratory tract functioning, teeth abscess and infections observed while a miniaturized version of the VNS device was deployed systematically. The procedure focused on the impact of the device's usage on the various individuals. The focus of the experiment was aimed to prove that the deployment of the device under non-epileptic situations will not affect the physiology of the patient adversely. The system was deployed with systemic time differences in voltage administration. The individuals were chosen based on classification of their unique physiological differences along with another set of individuals chosen arbitrarily. The inference corroborates the claim, but the success displayed is not absolute. The neuro-stimulation devices outcomes were studied but the device itself was not studied i.e., the working principles as well as operational contingencies were not addressed [11,12].

Another attempt at using biomarkers to detect and respond to epilepsy via blood pressure variables was studied. The idea was to use biometric information such as blood pressure spike during the onset of epilepsy

to trigger the IoT devices to dispatch alert messages to caregivers and medical personnel to attend the patient. The system functions like a personal threat response system but the system itself do not have any direct impact towards GTCS epilepsy treatment. The system addresses the problem of defenselessness a patient undergoes when loss of consciousness occurs during epileptic episode. The system observed the patient, but an analysis of device specific treatments was not addressed [13,14].

Rheumatoid arthritis (RA) was treated through Bioelectronic therapy (BET), such as electrical neuro-stimulation of the Vagus nerve to activate innate protective neuro-immune reflexes with positive results. The deployed system was a novel system that emphasized the applications of Vagus nerve on ailments other than epilepsy. The system showed success in alleviating RA symptoms with no device related complications observed. The cardiac safety of the Micro-regulator was documented by extensive ECG monitoring, via 12-lead ECGs, cardiac monitoring during stimulation dose escalation, and long-term ambulatory telemetry. No stimulation associated arrhythmias were noted during the study. Again, the device's impact on the body was studied while the device itself remains untested [15–17].

All references in regards to epilepsy state that the Vagus nerve has a direct relationship with heart, liver, stomach, and spleen through the nerves associated with the organs. These organs are responsible for the maintenance of living quality of a patient and if adversely affected will give rise to complications. This need to the address complications is aggravated in a person with GTCS epilepsy because a single epileptic episode renders the patient temporarily comatose.

### ***2.1 Working of a Traditional VNS***

Presently VNS is a standalone system that is surgically implanted into a patient's body that is similar in many ways to a pacemaker [18]. There is a pulse generator that is implanted in the thoracic cavity near the heart and the electrical leads are taken from that node to be fused into the left Vagus nerve. The right Vagus nerve is an immensely complicated nerve that is intimately associated with the heart. This is the reason for choosing the left nerve as the right nerve may lead to atrial fibrillation which may render the patient to suffer arrhythmia and in the worst case, it can go into a myocardial infarction (a.k.a. heart attack). As the left nerve handles delivering sensory information to the brain which represents the processing of all sensory data from the body, the leads of the Vagus Nerve Stimulation system are attached to it which counteracts the erratic electrical impulses and pulls the patient through epileptic seizures. The VNS system, when activated by the external wand, sends an electrical impulse of 10–25 V that counteract the seizure-inducing signals through the left Vagus nerve to the brain. These counter signals can be defined as a pulse of equal (approx) magnitude and opposite direction if expressed as a vector. Thus, the erratic signals from the brain are halted at the location of the VNS node.

Some ramifications including the toll taken on by the body from the erratic signals sent by the brain should be taken into account. Some of the officially released ones include coughing and shortness of breath and the more severe would be cardiac arrest. It is to be noted that the VNS system is deployed as a last resort to patients who are drug-resistant to anti-epileptic medicines.

### ***2.2 Risks of Vagus Nerve Stimulation***

The Vagus nerve stimulation device acts as a response gateway that blocks the incoming signal through counter action. This implies conflict and thus also implies casualties i.e., the nerve in question must take the load of two opposing electrical impulses which the nerve was not initially intended for. This implies that the nerve will come under duress every time the device is put in use. Thus, it needs to be used with caution.

The second implication is that the system is activated by an external entity (in most cases) with a magnetic wand. The external entity makes the decision based in his/her own judgment of the situation implying that the patient has no opinion/choice in the activation of the VNS system. False activation may

i) trigger seizure ii) affect the brain receptors of the Vagus nerve. The problem caused by the VNS device's unexpected activation is the focus of this paper. The paper proposes a solution that ensures the protection of the VNS system. By implementing integrity management protocols, the proposed solution would ensure that the VNS system is only enabled when absolutely necessary, ensuring secure use.

### 3 Proposed System

The motivation of the proposed system is that the experiments had no mention of operational safety parameters. The experiment did not address unforeseen activation of the device and the device itself had no safety guards to oversee its utility. The device is activated purely based on human decision making.

The system faces the problems of unexpected activation. The solution prescribed is to integrate a stand-alone system with an IoT device that monitors that patient to verify whether the patient requires the usage of the VNS system [19]. In addition, the IoT device has constant oversight by a third-party observer who monitors the systems and recommends due actions. If the system is activated, it must be accounted for by the oversight system and if an out-of-parameter activation occurs, proper response must be initiated and alerted automatically. The data acquired shall be used as a solid evidence for occurrence of such events to instigate further review of the incident for legal, medical and software augmentation purposes.

The proposed system is composed of the VNS device and a smart watch that monitors the blood pressure and pulse rate of the patient to establish nominal parameters. The second criterion is where his blood pressure and heart rate reading taken while the patient is under the effects of the epileptic episode. These readings are then uploaded to a private Blockchain where the data (both nominal and epileptic) is used for reference of activation [20]. The Blockchain is an open platform where the miners are the patients, the immediate caregivers (who has the magnetic wand) and the doctors (who oversees all the above). This ensures that the system is open only to the relevant people to preserve Doctor-Patient confidentiality [21,22]

#### 3.1 The IoT-VNS Working Principle

The first phase is to add a twin activation switch to the VNS system, so that it requires a “go” (positive authentication) from both the magnetic wand and the smart watch. The smart watch monitors the patient's vitals and if the readings fall out of nominal range, the smart watch sends the “go” signal while reporting the same to the Blockchain.

The system can be designed to have a smart contract, to verify the data, to issue another separate “go” signal but for real-time responses it is inadvisable as Blockchain's response time is incompatible. Since the design intention is for the device to be used safely, the Blockchain reporting mechanism will serve to make the system safe and secure. An IoT/Blockchain based VNS system is shown in Fig. 1.

The mechanism is similar to the two-factor authentication systems (2FA) found in safety deposit boxes wherein two keys are necessary to open the lock and the no of times the deposit box is opened is maintained by the repository [23,24]. The same principle is adopted here to ensure that only authenticated users may activate the VNS system.

The second step is to connect the activating magnetic wand to the IoT Smart watch via Bluetooth. The watch is embedded with proper authenticating mechanisms such as biometric fingerprint recognizer that identifies the patient or the immediate caregiver. This is to ensure that the wand is secure from mishap and to ensure utility only by the Blockchain authorized entities.

Collectively, the Smart watch acts as the focal point of observing the patient's vital status & the biometric wand usage is taken into consideration before giving the “go” signal for the VNS device as shown in Tab. 1.

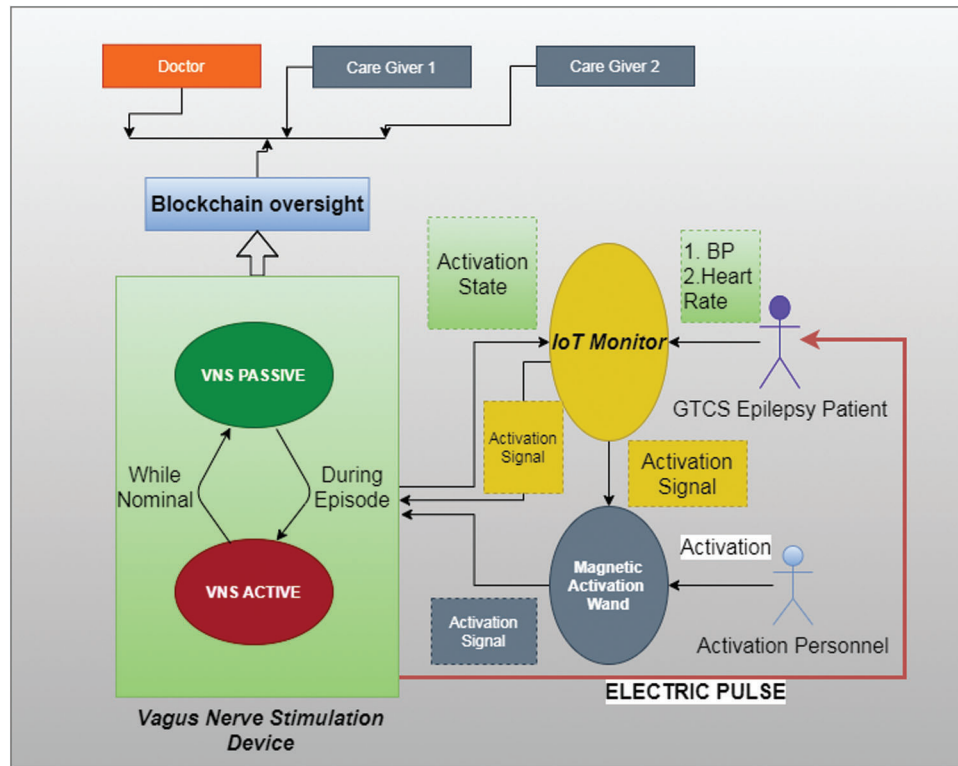


Figure 1: Proposed IoT/blockchain VNS architecture

Table 1: Scenario of VNS activation

S. no	Blood pressure	Pulse	Wand biometric	Status
1	Normal	Normal	Yes/no	No-Go
2	Normal	Beyond parameters	Yes/no	No-Go
3	Beyond parameters	Normal	Yes/no	No-Go
4	Beyond parameters	Beyond parameters	Yes	Go-VNS; Go-Wand

The VNS device activates only after receiving the “go” signal from the Smart watch and then activated magnetically. The “go” signal releases the lock for both the VNS device and the wand. Also, the presence of Blockchain ensures openness whilst at the same time, the occurrence of faults are nullified.

This critical factor separates the traditional VNS device from the IoT-VNS device making the system free from false activation. This phenomenon was observed in the Arduino based prototype that was assembled for study. The observations were deployed for the bio markers of the 18-year-old patient to obtain positive results.

### 3.2 Preprocessing Epilepsy Data Set

The nominal parameter of the patient was observed during non-epileptic situations to establish the nominal range of blood pressure and heart rate. This forms the data-set that defines the “idle” state of the

IoT-VNS device. When the bio marker exceeds 30% from the established norm to the zone of hypertension, the possibility of GTCS epilepsy is imminent.

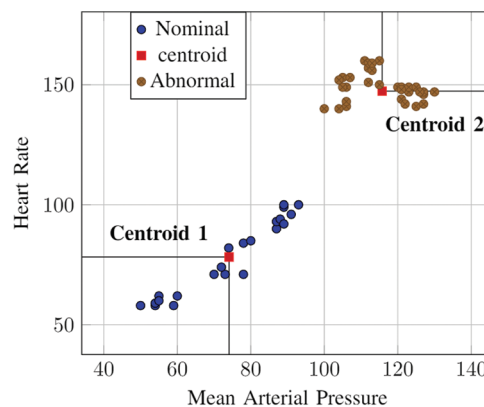
Clinicians argue that the nominal operation range of an adult male is 60 bpm to 100 bpm and the blood pressure range from 120/80 mmHg. This value was calibrated for the data-set of epileptic patients (both GTCS and non-GTCS) through the K-means algorithm.

The K-means algorithm was employed because the system requires data to be quantified in binary: i) Either the incoming biomarkers of the patient are in the nominal state, ii) or falls into the category of the epileptic state. The values of Heart rate and Mean Arterial Pressure are preprocessed to establish nominal parameters and abnormal parameters of bodily function shown in [Tab. 2](#).

**Table 2:** Establishing norms for blood pressure and heart rate

Category	Blood pressure	Heart rate	Activation
K-means nominal centroid value	74.091 mmHg	78.227 bpm	Opposed
Clinical nominal	70–100 mmHg	60–100bpm	Opposed
K-Means epileptic centroid value	115.742 mmHg	147.355 bpm	Endorsed

Through K-means, the nominal operating parameters for epileptic patients are established. [Fig. 2](#) depicts the usage of K-means centroid based clustering to identify nominal threshold. The results show that the nominal heart rate varies by about 31.17% & blood pressure varies by about 5.84% for epileptic patients. The abnormal range differed by 47.6% for heart rates and 15.74% for blood pressure from the established norm. This baseline is used as a delimiter to classify the current state of the patient. This value is used to establish the “go” and “no-go” signals for system design in the subsequent chapters.



**Figure 2:** KNN: nominal value establishment

### 3.3 The Implications of IoT Addendum

Here, the nominal values established by K-means clustering acts as a demarcation criteria for the system to classify critical vitals from nominal vitals. Algorithm 1 is a mutually exclusive operating system that provides a secure environment for the device to function. The variables “VNSwand” and “SmtWatch” are binary variables that operate together to ensure safety of the device. They both need to be in the “ON”

state for the VNS system to be active. This establishes the two-man activation system the IoT device is based on [24].

---

**Algorithm 1:** Activation of Failsafe Algorithm
 

---

Result: VNS Activation and Report generation

```

initialization;
VNSstate←false; SmtWatch←Nominal; VNSwand ← inactive; BC←Blockchain/Smart Contract
while Active do
    Activation(VNSwand, VNSstate)
    if VNSwand == active && SmtWatch ≠ Nominal
    Then
        |           VNSstate ← true & VNSwand ← active
        |           Call BC_trigger(VNSstate, VNSwand)
    else
        |           VNSstate ← false & VNSwand ← inactive
        |           Call BC_trigger(VNSstate, VNSwand) /* Report Anomalous Incident*/
    end
    UnintentionalActivation(VNSwand, VNSstate)
    if VNSwand ≠ active && VNSstate ← True && SmtWatch ← Nominal
    Then
        |           VNSstate ← true & VNSwand ← active
        |           Call BC_trigger(VNSstate, VNSwand)
    End
End
  
```

---

The function Activation () is designed to address the cases of activation of the VNS device for medical reasons and addresses the event of malicious activation. The function, as mentioned above, utilizes dual binary variable state synchronization, “VNSwand” and “SmtWatch”, to initiate activation. These dual variables must be boolean “true” to be activated.

The SmtWatch corresponds to the patient's symptoms detected in real time, prohibiting forgery. The VNSwand is connected directly to the SmtWatch. This means that the reliability of the SmtWatch is directly connected to the VNSwand. Additionally, the VNSwand must be physically activated, granting an added layer of security for the variable independent of the SmtWatch variable. The variables are outlined in [Tab. 3](#).

The function Unintentional Activation(), in Algorithm I, is designed to address the contingency of unintentional activation. The instances where the patient is exposed to an MRI machine or security checks at the airport using an RF wand, where patient is exposed to an oscillating magnetic field may trigger the VNS device. The two-point fail-safe through IoT device makes the system impregnable. The probability of occurrence of the event as a standalone system is 0.5. Whereas the probability of the same

event occurring in the proposed system is 0.3 and that is only under the criteria that all three interconnected devices, i.e., the smart watch, VNS node and the magnetic wand, are compromised [25].

**Table 3:** Variables used in the algorithm

Variable	Boolean state oscillations	Description
VNS state	True/false	The current State of the VNS embedded device. Responds to “go” signals from the smart watch and magnetic wand.
SmtWatch	Nominal/nominal	Smart watch monitor that consolidates the vitals into a single variable “Nominal” or otherwise.
VNSwand	Active/inactive	This is the activation wand of the VNS device It needs two-man activation from the caregiver and Smart watch.
Bctrigger	Connected/disconnected	This is a communications variable that triggers the report generation of the decision made by the VNS system.

#### 4 IoT-VNS and Blockchain Smart Contract

As stated above, an 18-year-old patient with myoclonic epilepsy is considered for study, to establish baseline parameters for nominal operation of the IoT based VNS device, while Blockchain smart contracts provide third-party verification. The patient was recorded to exhibit the following vitals before, during and after the onset of a clonic seizure episode.

From Tab. 4 it can be inferred that the patient, while suffering from the onset of clonic seizure that causes unconsciousness, is experiencing a 30% increase in blood pressure due to the erratic triggers from the brain. This 30% variation observed during epileptic episodes can be utilized as a threshold for the authentication of the IoT-VNS device. The proposed system is a 2FA authentication system that verifies a trigger made by a human caregiver through patients’ ongoing vital status. This implies that the system requires defined parameters to operate on.

**Table 4:** Patient vitals before and under duress of epileptic seizure

Patient state	MAP	SBP	DBP
Nominal phase	81 mmHg	98 mmHg	69 mmHg
Clonic phase	94 mmHg	209 mmHg	36 mmHg
Suppression phase	41 mmHg	48 mmHg	34 mmHg

##### 4.1 Activation Threshold Establishment

The “SmtWatch” is the variable that oversees the blood pressure of the patient to directly validate the physical condition of the patient. In the scenario where the patient is going into clonic seizure the patient will exhibit a MAP value [26] of  $\pm 94$  mmHg and not under other circumstances. Therefore, the values  $>93$  mmHg is used as the “go” signal that is generated by the Smart Watch.

$$MAP = (SBP + 2 * DBP)/3 \quad (1)$$

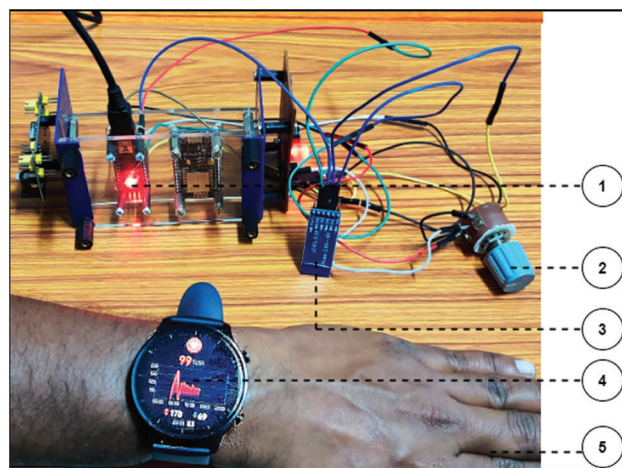
where, SBP represents Systolic Blood Pressure, DBP represents Diastolic Blood Pressure and MAP Mean Arterial Pressure.



Any value under the threshold is the nominal “no go” state that makes the VNS system remains in stand-by mode. MAP is a value arrived from the expression stated in Eq. (1) the device need only respond to the state of MAP being beyond threshold.

#### 4.2 IoT-VNS Prototype

An experimental prototype specified in Fig. 3 was developed using Arduino Nano IoT board and a RF signal generator that served as the IoT observer that monitor the patients’ blood pressure parameters continuously [27]. This is because an actual IoT based VNS system requires approval by the “Drugs Controller General of India” (DCGI) under “Central Drugs Standard Control Organization” (CDSCO). The prototype observes the following specifications [28–30].



1. ARDUINO CONTROLLER      4. SMART WATCH  
 2. POTENTIOMETER              5. HUMAN SUBJECT  
 3. BLUETOOTH INTERFACE

**Figure 3:** Proposed working model: IoT-Blockchain VNS Device

The processor utilizes a state change algorithm that simulates the patients’ MAP value from nominal to clonic to suppressed phase in a cyclic pattern. The manual activation representing the caregiver is done through GUI based direct user input which is recorded and transmitted to the private Blockchain via Wi-Fi. The RF signal generator represents the VNS system that will be activated if the two-man system is in agreement. The private Blockchain is triggered only under abnormal activation.

#### 4.3 Prototype Inferences

The following are the observations gained from the IoT-VNS prototype after 87 iterations of varying blood pressure from nominal  $<94$  mmHg to clonic  $\geq 94$  mmHg. Suppressed phase need not have medical intervention [30,31].

The system that can be activated randomly by user/caregiver is completely mitigated. Abnormal activations have been documented as a new block in the private Blockchain. The patients’ seizure status is monitored continually (in experimentation) as the smart device is programmed with the seizure protocol of the patient specifically.

Patients' unconscious states may also be alerted for safety reasons through programming.

#### 4.4 The Blockchain Component

The Blockchain component is utilized as a mechanism to ensure reliability to the system throughout the utility of the device by the patient. The Blockchain component is deployed as a third-party observer that monitors the progress of the system periodically. Here, we use an Ethereum based private Blockchain to check that the device runs at specified parameters only. The IoT-VNS device will generate a report having the following: i) Blood Pressure (MAP, SBP, DBP), ii) Heart rate, iii) State of Device (Active/Inactive).

This report will be sent to the Blockchain as per the smart contract between the IoT-VNS device and the Blockchain. The data can only be sent at 8-hour intervals, in the absence of abnormal activation, and added as a block in the chain. The data will be encrypted with the primary miners' id so that the block can be verified and added to the chain. In the proposed model the patient i.e., the IoT-VNS device and the doctor and two assistants are miners. It considers the state of operations the IoT-VNS device goes through, and maintains a record of it. Algorithm 2 shows the operating protocols of the Blockchain module.

---

#### Algorithm 2: Module: Report Generation Smart Contract

---

**Result:** New Block containing Patient Data

initiation:

New Block Report(VNSstate, VNSwandd)

MAP ← VNSstate MAP; HR ← VNSstate HR

**if** VNSwand == active && SmtWatch = Nominal

**Then**

    Manual\_Activation: goto step 13

**Else**

    clock ← func(unix time, 28800sec) /\* *unix\_time\_to\_real\_time* \*/

**while** 8 h clock intervals **do**

        New\_Block\_Create (MAP, HR, VNSwand)

**End**

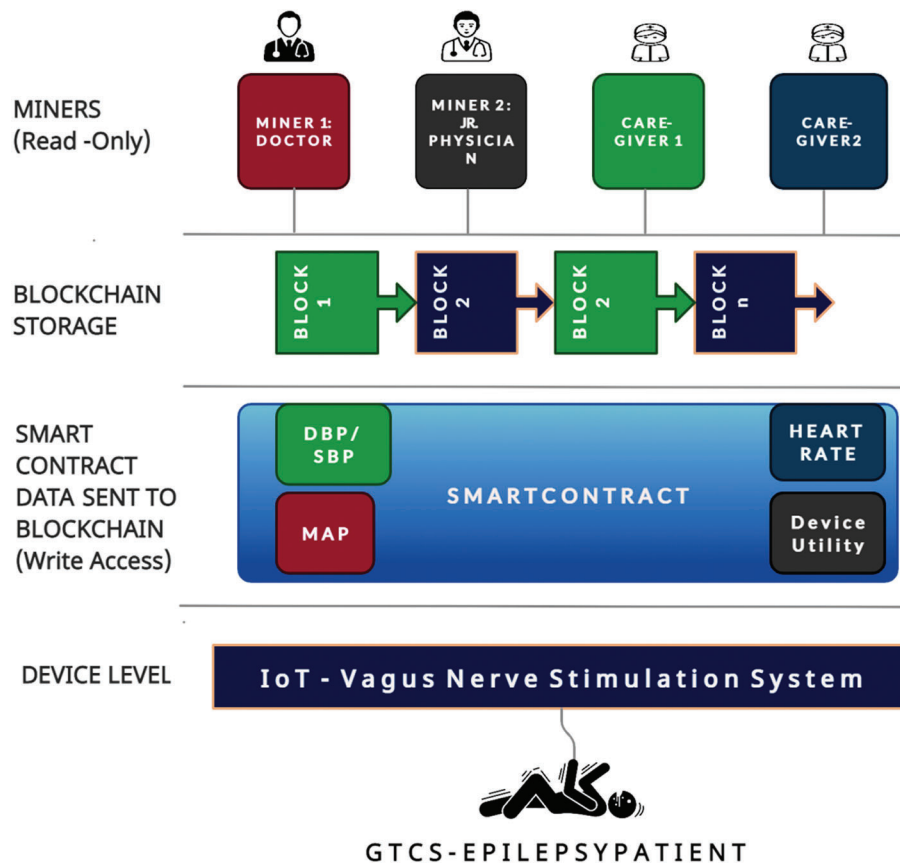
**end**

---

This data can be used to discover patterns in the recurrence of the epileptic episodes. The system, depicted in Fig. 4, is designed to directly create a new block when the system forcibly halts the activation of the device as it had detected abnormal activation. This is to ensure that the abnormal activation has an off-device counter copy that can be used for device analysis and legal purposes if necessary.

The inclusion of IoT and Blockchain addresses the following security threats to the Epileptic patient whilst being under the influence of the VNS system. 1) The patient is currently well but an unexpected activation of VNS. 2) Case Scenario 2: Accidental Activation of VNS. In these situations the system will fail to trigger VNS nodes because the system is not within the emergency parameters monitored by the smart watch. The smart contract algorithm utilized to create a new block in the chain is shown in Algorithm 2.

The legal purposes necessitate the presence of Blockchain Smart contracts as they are immutable. The architecture is shown in Fig. 4.



**Figure 4:** Architecture of Blockchain based IoT-VNS device

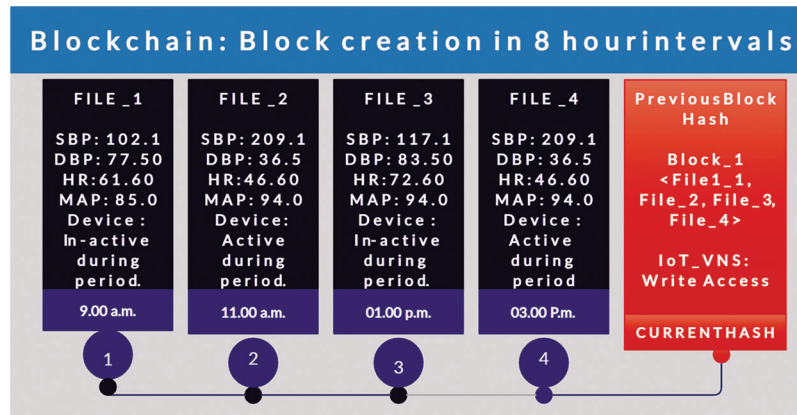
The various factors of Blockchain and smart contracts that were retrofitted to represent a medical report are outlined below.

#### 4.4.1 Patient Stakeholders' Privileges

The patients' IoT-VNS device: The device is worn by the patient will be assigned a unique ID through which it will create new blocks onto the Blockchain every 8 h. This block will have information on the average MAP, SBP, DBP, heart rate, device activation information, time of activation during the 8-hour cycle from the previous block as shown in Fig. 5. A random block will be generated only during activation under abnormal situations. The data from the device is sent to the Blockchain via smart contract. The contract will explicitly state what data should be uploaded onto the chain so that the purpose of monitoring is valid in both medical and security contexts.

#### 4.4.2 The Doctor/Caregiver

The caregiver will be granted viewing privileges only. Since the Blockchain serves as proof of the events surrounding the patients' vitals, the doctor does not need to contribute any details. The Doctor, as the principal caregiver, needs only to investigate the Blockchain and adjust device parameters at the next appointment of the patient. The Doctor can obtain a complete workup of the treatment given to the patient and ensure conformance of medication. If the Doctor needs to upgrade the prescription, a new one can be added as a block onto the private chain. The older prescription remains undisturbed for future reference. No remote login or control is considered as specific care is needed for GTCS epilepsy.



**Figure 5:** Architecture of Blockchain based IoT-VNS device

#### 4.4.3 The Consensus Mechanism & Miner Appointment

The Blockchain technology demands that a new block to be added must be a miner who has access to the Blockchain. A new miner will be chosen by various algorithms such as PoW, PoS, PBFT, and DPOS. But for the sake of operational simplicity, we chose to deploy a static Blockchain that has fixed miners assigned to it. As previously mentioned, the patients' IoT-VNS computer is registered as a miner in the Blockchain and given a unique identifier. The device uses that ID as a Blockchain identity to "write" new blocks into the chain. Here no election mechanism is used, as only the data generated by the device implanted in the patient will be uploaded to the Blockchain as a smart contract.

The remaining miners for the Blockchain with viewing privileges are Junior Doctors and caregivers. A principal miner is appointed, and they are in charge of continuously monitoring the chain. In the absence of the principal miner, the other caregivers elect a new miner. The most active miner among the other caregivers will be assigned as the principal miner, and per the election specifications.

Since the Blockchain used is a private static Blockchain that is not built for scalability, the conventional consensus miner election and Proof-of-Work are not used. The number of miners with viewing access permissions is limited and there is only one miner who can write new blocks onto the chain. As such, the traditional implementation of Block chain is in systems like Bitcoin which are unnecessary as it is too computationally intensive and requires a multitude of resources. The smart contract is needed only on the patient side as it is the only miner that generates new blocks.

#### 4.4.4 Data Validity

The stored data is in the form of a Blockchain and as such the blocks need to be shared among the various miners for scrutiny. Presently, the prototype data is made to be valid throughout the lifetime of the IoT-VNS device so that medical analysis may be carried out. But it is recommended to scrap data periodically to keep the storage needs of the Blockchain to a smaller scale. Presently, if a single Blockchain data for a period of 10 days (about 1 and a half weeks) needs 1GB worth of storage space and if at least four miners are involved (irrespective of access permissions) then a grand total of 4GB storage space is needed to keep four individual copies of Blockchain. This requirement will grow exponentially if larger timelines are stored. For smaller monitoring systems with limited oversight, a typical 30-day cycle is recommended, with periodic data consolidations. For data protection, copies of anomalous data are provided to the patient.

#### 4.4.5 The Time Component

The smart contract for the Blockchain is deployed via Ethereum, an open-source forum that can serve as base to compose and deploy smart contracts. The language used is called “Solidity” through which the smart contract prototype was reconfigured to handle medical data from IoT devices rather than just transact “Ether”—the currency of Ethereum. The medical system proposed runs perpetually with 8-hour cycles of data generation. But solidity runs based on “UNIX EPOCH” time, an abstract counter-based measurement of digital time that returns the current “time” value in seconds. Thus, the IoT-VNS device needs to be reconfigured to implement real-time counter via Unix Epoch time. The Unix Epoch time can be accessed by the command “block.timestamp()”.

The command can be used to access the current value of Epoch time and from that point in time, the 8-hour duration cycles can be achieved as a temporal function of the current time multiplied by 28800 s (8 h). This creates an alarm-like function that triggers the transfer of data from the IoT-VNS device. The proposed smart contract algorithm consumes a “Gas” currency of 23546 gas. Thus, the present prototype system spends more Gas currency values which is eliminated when deployed over a private, static, and simplified Blockchain mechanism.

## 5 Results and Discussions

The system was trained based on the input of a 281 [10] unique values of Blood pressure and heart rate gathered from GTCS epileptic patients during pre-epileptic period. The spike in blood pressure and pulse was also calculated and fed into the Arduino prototype. The data from the smart watch was fed into the device and it was seen that the system responded only to values that were beyond the safe threshold range. All values below the range were ignored and the system remained in idle observation state. The range of training inputs are is shown in [Tab. 5](#).

**Table 5:** Testing dataset-standalone vs. IOT-VNS observations

Expected state	SBP	DBP	MAP	HR	Traditional	Proposed	Revised
Idle state	70	40	50	58	13	0	Optimized corrections in IoT-VNS
	80	50	60	62	20	0	
	90	60	70	71	11	0	
	100	70	80	85	20	0	
	110	75	87	90	19	0	
	120	80	93	100	20	0	
Active state	130	85	100	140	19	18	Redundant
	140	90	107	153	12	12	
	150	91	111	160	25	25	
	160	92	115	150	13	13	
	170	35	120	149	24	24	
	180	97	125	141	12	12	
	190	100	130	147	12	12	

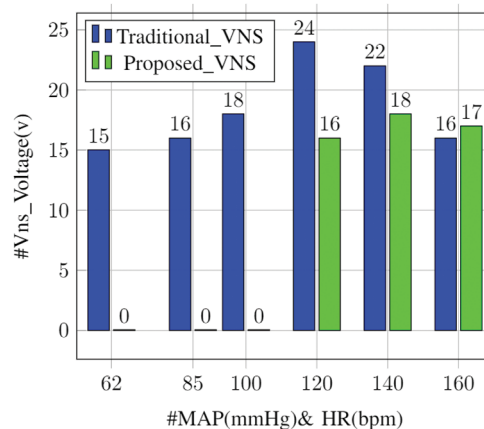
Inference: IoT mitigates false activation by 46.2%

The Arduino prototype was fed an additional ON/OFF binary parameter to simulate the manual intervention of the Activation wand. The system was tested under both nominal and abnormal biometric values. It was observed that the standalone system could be activated regardless of the patient's ongoing epileptic status while the proposed system did not activate due to opposing smart watch data.

The trained system was tested against the dataset of the 18-year-old GTCS epileptic patient and the system was made to iterate for 30 min. The system showed that the Arduino prototype would only activate the electrical actuator only for data's that corroborate with the patient's epileptic state. The system remained inactive as the smart watch data acted as a delimiter to the prototype.

The system generated reports having the data was uploaded onto the Blockchain after 1800 Unix clock time intervals rather than 28800 clock intervals. This revision corresponds to the 30 min period the prototype was tested against. The smart contract upload was simulated on Remix-Ethereum IDE. The overall report generation cost 114939 gas units and 112867gas units for execution.

The failure of the standalone device was observed to be a value of 46.2% for the 281-patient dataset it was iterated against. This drawback has been completely overcome by the proposed IoT-VNS device. Fig. 6 outlines that the proposed system was able to successfully delineate when the VNS system should operate, which is absent in the traditional system. The device showed complete operational accuracy for the training dataset. Further testing is required to arrive at the final report but presently for the vitals of the 18-year-old patient under study the IoT-VNS system shows to provide greater security than the standalone counterpart.



**Figure 6:** Activation comparison: standalone vs. IoT VNS

## 6 Conclusion

The present Vagus Nerve Stimulation (VNS), because of its stand-alone design, required a safeguard addendum to protect the patient's life. This can be interpreted as a possible entry point for an anomalous agent to threaten the patient's safety and security. The design presents an Internet of Things (IoT) and Blockchain-based oversight framework that can be used to ensure that the system is used correctly with validation. The system is made up of three components: the VNS unit, the Smart watch, and the activation wand. To activate the epilepsy mitigation unit, the systems of the Smart watch and the Wand coordinate with one another. The Blockchain monitoring system keeps track of the system's openness and accountability. The simulator has reiterated that the solution is viable. When compared to a standalone system, the prototype implementation substantiates the principle of ensuring security. Future studies will concentrate on reducing the productivity loss caused by Blockchain incorporation.

**Funding Statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

- [1] K. Myers, S. Sivathamboo and P. Perucca, "Heart rate variability measurement in epilepsy: How can we move from research to clinical practice?," *Epilepsia*, vol. 59, no. 12, pp. 2169–2178, 2018.
- [2] H. Luan and Y. Zhang, "Programmable stimulation and actuation in flexible and stretchable electronics," *Advanced Intelligent Systems*, vol. 3, no. 6, pp. 2000228, 2021.
- [3] M. Nei, "Cardiac effects of seizures," *Epilepsy Currents*, vol. 9, no. 4, pp. 91–95, 2009.
- [4] G. Sainas, R. Milia, G. Palazzolo, G. Ibba, E. Marongiu *et al.*, "Mean blood pressure assessment during post-exercise: Result from two different methods of calculation," *Journal of Sports Science and Medicine*, vol. 15, no. 3, pp. 424–433, 2016.
- [5] A. Bozorgi, C. Stephanie, K. Farhad, A. Kenneth, S. S. Loparo *et al.*, "Significant postictal hypotension: Expanding the spectrum of seizure-induced autonomic dysregulation," *Epilepsia*, vol. 54, no. 9, pp. e127–e130, 2013.
- [6] K. Hampel, A. Jahanbekam, C. Elger and R. Surges, "Seizure-related modulation of systemic arterial blood pressure in focal epilepsy," *Epilepsia*, vol. 57, no. 10, pp. 1709–1718, 2016.
- [7] R. Nass, K. Hampel, C. Elger and R. Surges, "Blood pressure in seizures and epilepsy," *Frontiers in Neurology*, vol. 10, pp. 501, 2019.
- [8] M. Zijlmans, D. Flanagan and J. Gotman, "Heart rate changes and ECG abnormalities during epileptic Seizures: Prevalence and definition of an objective clinical sign," *Epilepsia*, vol. 43, no. 8, pp. 847–854, 2002.
- [9] M. Ali, M. Abdelwahab, S. Awadekreim and S. Abdalla, "Development of a monitoring and control system of infant incubator," in *Proc. in 2018 Int. Conf. on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*, Sudan, pp. 1–4, 2018.
- [10] X. Li, X. Peng, M. He, R. Wang and J. Guo, "Design of portable transcutaneous vagus nerve stimulator based on microcontroller," in *Proc. 2018 12th IEEE Int. Conf. on Anti-Counterfeiting, Security, and Identification (ASID)*, China, pp. 231–235, 2018.
- [11] M. Genovese, G. B. Norman, S. David, K. Alan, L. H. Diane *et al.*, "Safety and efficacy of neurostimulation with a miniaturised vagus nerve stimulation device in patients with multidrug-refractory rheumatoid arthritis: A two-stage multicentre, randomised pilot study," *The Lancet Rheumatology*, vol. 2, no. 9, pp. e527–e538, 2020.
- [12] D. Zeng, Y. Hu, Q. he, B. leng, H. wang *et al.*, "Study of intelligent bio-feedback therapy system based on transcutaneous electrical nerve stimulation and surface EMG signals," in *Proc. 2013 IEEE Int. Conf. on Information and Automation (ICIA)*, China, August, pp. 337–362, 2013.
- [13] S. Tiwari, V. Sharma, M. Mujawar, Y. Mishra, A. Kaushik *et al.*, "Biosensors for epilepsy management: State-of-art and future aspects," *Sensors*, vol. 19, no. 7, pp. 1525, 2019.
- [14] P. Bizopoulos, D. Tsalikakis, A. Tzallas, D. Koutsouris and D. Fotiadis, "EEG epileptic seizure detection using k-means clustering and marginal spectrum based on ensemble empirical mode decomposition," in *Proc. 13th IEEE International Conference on BioInformatics and BioEngineering*, Greece, pp. 1–4, 2013.
- [15] D. Chernoff, Y. Levine, C. Peterfy and M. C. Genovese, "A First-in-man bioelectronic therapy for biologic-refractory rheumatoid arthritis," March, pp. 1, 2021 [Online]. Available: <https://web.archive.org/web/20201027101752/https://acrabstracts.org/abstract/a-first-in-man-bioelectronic-therapy-for-biologic-refractory-rheumatoid-arthritis>.
- [16] P. Kapen, Y. Mohamadou, F. Momo, D. Jauspin, N. Kanmagne *et al.*, "Development of a neonatal incubator with phototherapy, biometric fingerprint reader, remote monitoring, and heart rate control adapted for developing countries hospitals," *Journal of Neonatal Nursing*, vol. 25, no. 6, pp. 298–303, 2019.
- [17] A. Shabeeb, A. Al-Askery and Z. Nahi, "Remote monitoring of a premature infants incubator," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1232, 2020.

- [18] J. Li and Y. Sawanoi, "The history and innovation of home blood pressure monitors," in *Proc. 2017 IEEE History of Electrotechnology Conf. (HISTELCON)*, Japan, pp. 82–86, August, 2017.
- [19] R. Ranjandish and A. Schmid, "Implantable IoT system for closed-loop epilepsy control based on electrical neuromodulation," in *Proc. 2018 IFIP/IEEE Int. Conf. on Very Large-Scale Integration (VLSI-SoC)*, Italy, pp. 155–158, 2018.
- [20] F. Loukil, C. Ghedira-Guegan, K. Boukadi, A. Benharkat and E. Benkhelifa, "Data privacy based on IoT device behavior control using blockchain," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–20, 2021.
- [21] M. Alamri, N. Jhanjhi and M. Humayun, "Blockchain for internet of things (IoT) research issues challenges & future directions: A review," *International Journal of Computer Science and Network Security*, vol. 2019, pp. 244–258, 2019.
- [22] A. P. Singh, N. R. Pradhan, A. K. Luhach, S. Agnihotri, N. Z. Jhanjhi *et al.*, "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5779–5789, 2021.
- [23] J. Qu and X. Tan, "Two-factor user authentication with key agreement scheme based on elliptic curve cryptosystem," *Journal of Electrical and Computer Engineering*, vol. 2014, pp. 1–6, 2014.
- [24] C. Chen and C. Lee, "A Two-factor authentication scheme with anonymity for multi-server environments," *Security and Communication Networks*, vol. 8, no. 8, pp. 1608–1625, 2014.
- [25] E. Letier, D. Stefan and E. Barr, "Uncertainty, risk, and information value in software requirements and architecture," in *Proc. of the 36th Int. Conf. on Software Engineering*, United States, pp. 883–894, May, 2014.
- [26] A. Grillo, P. Salvi, G. Furlanis, C. Baldi, M. Rovina *et al.*, "Mean arterial pressure estimated by brachial pulse wave analysis and comparison with currently used algorithms," *Journal of Hypertension*, vol. 38, no. 11, pp. 2161–2168, 2020.
- [27] L. Li, Y. Li, L. Yang, F. Fang and Q. Sun, "A wearable optical fiber wristband for continuous and accurate blood pressure monitoring," in *Proc. Conf. on Lasers and Electro-Optics*, USA, pp. 1–2, 2020.
- [28] W. Shalannanda, I. Zakia, E. Sutanto and F. Fahmi, "Design of hardware module of IoT-based infant incubator monitoring system," in *Proc. 2020 6th Int. Conf. on Wireless and Telematics (ICWT)*, Yogyakarta, September, pp. 1–6, 2020.
- [29] A. Sharma, T. Choudhury and P. Kumar, "Health monitoring and management using IoT Devices in a cloud based framework," in *Proc. 2018 Int. Conf. on Advances in Computing and Communication Engineering (ICACCE)*, France, June, pp. 219–224, 2018.
- [30] T. Khan and M. Chattopadhyay, "Smart health monitoring system," in *Proc. 2017 Int. Conf. on Information, Communication, Instrumentation and Control (ICICIC)*, India, August, pp. 1–6, 2017.
- [31] S. Beniczky, A. Arbune, J. Jeppesen and P. Ryvlin, "Biomarkers of seizure severity derived from wearable devices," *Epilepsia*, vol. 61, no. 1, pp. S61–S66, 2020.