Grenze International Journal of Engineering and Technology, June Issue

IoT-Blockchain based Instrument Integrity Management System Deployed over Insulin Dispensary Device to Ensure Safe Utility

Karthikeyan G[1], Kousalya G[2] and Balakrishnan P[3]
[1-2]Coimbatore Institute of Technology / Computer Science Engineering, Coimbatore, India
Email: kousir@gmail.com karthikeyan.g14@gmail.com
[3]Vellore Institute of Technology/School of Computer Science and Engineering, Vellore, India
Email: baskrish1977@gmail.com

***Abstract*—IoT based Insulin pumps are utilized to deliver precise quantities of insulin to diabetic patients to regulate blood glucose levels. These levels correspond to the dietary patterns observed at time intervals that vary across patients. Precise representation of insulin in accordance to prescription is crucial. As such, most IoT based insulin pumps must be reinforced to endure external attacks. This includes software attacks and hardware attacks. One solution offered by the paper involves integrating Blockchain technology to ensure immutability to all instructions transmitted to the IoT Insulin pump. The second is a state-behaviour based solution that detects anomaly in the behaviour of the pump via temporal data resulting in halt of dosage. The proposed solution is successfully detects deviation in dosages ensuring safe utility.**

***Index Terms*— Internet of Things (IoT), Blockchain, Immutability, UPPAAL.**

I. INTRODUCTION

The paper aims at augmenting a medical actuator running on preset temporal programs with IoT (Internet of Things) technology successfully. It was recommended to augment IoT with a medical actuator with external threat detection and response systems to ensure safety [1–3]. The vulnerabilities of IoT system, such as authentication failure or loss of integrity, must be overcome to ensure safety of the patient. There is also a possibility of system failure due to external agents [4–6] and the attacker can simply wait for the actuator to execute a contradictory code while being physically anywhere. In this paper, an endeavor at integrating an Insulin Pump with an IoT processor is attempted. Blockchain technology is designed to be an immutable source of data that can be accessed by legitimate users without losing accountability. Since Blockchain technology requires time to complete traditional functionalities, behaviour analysis is deployed as anomaly detector for immediate responses and long term policy revision. Summary: The paper is divided into 6 sections. Section 1 a brief outline on traditional insulin pump and its cons. Section 2 and 3 discusses scenarios when IoT/insulin pumps are deployed. Section 4 will discuss Blockchain's role in the securing of IoT. Section 5 describes the mathematical substantiation of propositions. Section 6 Consolidates the contributions of proposed solution towards medial IoT devices.

Grenze ID: 01.GIJET.8.2.8_1

II. The Insulin Pump

The insulin pump is a medical device that is designed to deliver insulin to patients suffering from Type 1 or Type 2 Diabetes Mellitus [7]. The system is designed to deliver insulin based on a logic specifically tailored to the patients' degree of ailment. At the core of the system is a processor that oversees the actuator mechanism that delivers the insulin to the blood stream via catheter. The delivery mechanism has two different functionalities i.e. the basal rate and the bolus rate delivery. These deliver light doses and heavy doses as prescribed by medical practitioner. The outcome of these devices eventually leads to a balance in the blood sugar present in the individual [8]. These devices are based on preset programs fed into the system based on manual findings of blood sugar. The adjustments are made manually or via wireless access. Additionally the patient is expected to wear the device having limited knowledge of system accuracy. The only indicators are 1) Patient glucose measurements 2) If the person is able to function in a relatively normal fashion. The pump is an actuator controlled by a processor without an active sensor. This paper attempts to mitigate restrictions by monitoring situation through device behavior analysis and inconsistencies.

A. IoT augmented insulin pump

The IoT enhanced Insulin pump can directly communicate with a node (Laptop, Smart Phone etc.) via internet for a range of purposes including but not limited to data collection, program adjustment, device monitoring and patient status. The device can be monitored in real-time on patients who depend on it to sustain normalcy. The IoT enhancement required redress of security concerns of circumvention to violate norms stipulated on the medical device to ensure safe and secure usage [9–11]. The security bypass risk in IoT insulin pumps have significant consequences ranging from a loss of Quality of Life (QoL) to loss of consciousness. The outcomes of an unauthorized access are listed as 1) the dosage is increased resulting in extreme decomposition of blood glucose. Nominal result: Fatigue, Extreme cases: Loss of consciousness. 2) The dosage is decreased resulting in build-up of glucose, leading to Hyperglycemia. Nominal result: shortness of breath and nausea. Extreme cases: Cardiovascular Problems. 3) The dosage dispersal frequency becomes chaotic. Result: Varies from patient to patient.

Other complications include, insulin variations causing the patient to become unresponsive to insulin. In addition to the medical reasons, the data related to the patient may be obtained for study without patient consent. This is a critical factor that high profile patients demand in addition to personal.

III. The Insulin Pump's Working And Limitations

Figure 1 is a state transition diagram that will describe how an insulin pump works under uninterrupted normal circum- stances. Here, the patients' glucose status is monitored and appropriate actions are taken based on glucose variation and temporal data of food intake. All insulin pumps must consider four working conditions for nominal operations. The situations to be addressed as outlined in Table I. The categories are Basal – Nominal amount of insulin injected periodically and Bolus – Heavy dosage of insulin; to be initiated by patient. Limitations: The pump needs human intervention to intimate meal times and rise in blood sugar traditionally. IoT based pumps are limited as there are no sensors to initiate either cases.

Table I: Scenario of Patient Status and Response

S.No	Meal time	B.Sugar threshold	Outcome	Duration	Programmable Factor
1.	Yes	Excess	Bolus	1-4 hours	Insulin Quantity
2.	No	Excess	Bolus	Until Asymptomatic	Insulin Quantity
3.	No	Nominal	Basal	Periodic	Quantity and Frequency
4.	Yes	Nominal	Nil	Recovery Imminent	Abstinence

A. The IoT Insulin Pump

Legitimate IoT devices must have the following components [12, 13]. The Sensor / Actuator: An instrument that influences the real world, either by collecting data or by effecting quantifiable change. In the case of insulin pump the motor, piston and cannula together form the insulin delivery actuator. The Processor: The device housing insulin delivery pro- gram and executing it. The Battery: The power source that runs the device. The Communication module: IoT pumps can have wired and wireless communication links (BT-WiFi, BLE and ZigBee). The primary vulnerabilities recognized were present in the communications module that detriment the processor compromising the rest in a cascading fashion.

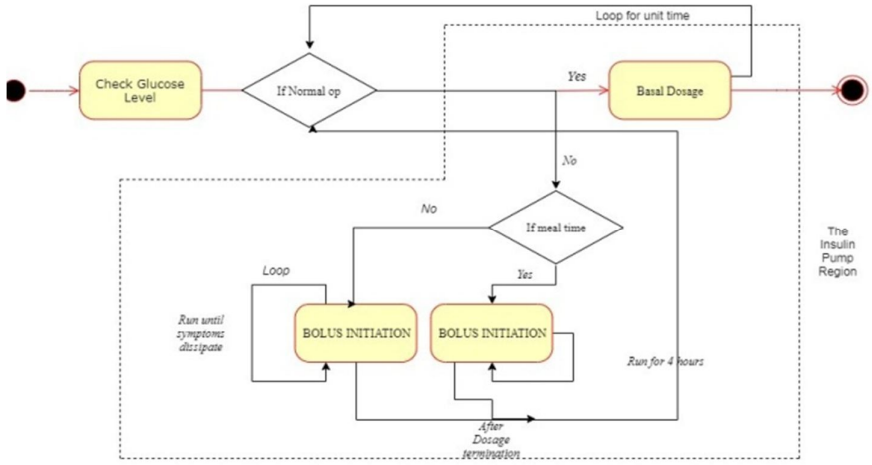

Figure 1. Working of an Traditional Insulin Pump – Uneventful Status

B. Possible attacks mounted against IoT Pump

The attacks that can be deployed against the IoT Insulin pump can be from the point of hardware i.e. physical sabotage or via software wherein the loaded program and communication ports are targeted to operate beyond intended parameters. Nearly all malfunctions result in loss of trust. The primary integrity affecting factors are software oriented attacks granting external entity to maneuver. Attacks on the IoT pumps include the following: 1) Denial of Service: Pumps re-programmed to continuously hoard processing time. Result: Device unusable. 2) Man-in-the-Middle attack: Communication port integrity loss results in device unreliablility. 3) Passive Attacks: Unauthorized personnel passively monitor the device & patient without consent. 4) Hardware attack: Tamper with piston or cannula hindering therapy delivery.

C. The Problem of trust

An attack on an IoT monitoring system has resulted in a loss of trust in the system. The external authority was able to reproduce credentials in a manner that met the systems' authorization parameters. The system lacks override mechanism that shuts down the pump once an anomaly is detected.

IV. The Blockchain – A Solution to Achieve Trust

Blockchain technology provides immutable accountability through redundancy as a part of its storage and transmission protocols [14, 15]. Immutability is achieved through irreversible hash values that link one block to the other. The redundancy exists so that if a corruption incurs the uncorrupted nodes will render it void. Presently, in order to corrupt an existing block chain 51 percent of all the miners must act together to achieve it. This is virtually impossible as the identities of the miners themselves remain masked by Blockchain protocol. Secondly, the cost of breaking the Blockchain is less rewarding than actually being a legitimate part of the distributed ledger network. Thus, the point of trust being established by Blockchain is considered a given in this work and a solution for IoT insulin pump is proposed as follows.

A. Blockchain- The Undeletable Blocks

The Blockchain mechanism is an immutable ledger that stores all transactions without deletion. Even if a subsequent block in the Blockchain contradicts the information contained in an earlier block in the chain, the older block is not terminated from the chain [15]. The new one is considered an update of the older chain and the older chain stands as evidence of earlier transactions.

The principal factor is accountability. The system holds itself responsible for all the data it broadcasts to its nodes in the distributed architecture. This factor helps in assessing the legitimacy of the data in question i.e. the Blockchain network must stand above reproach. Any two entities that verify any block at any point in time must find the same 1) Data 2) Previous Hash 3) Current Hash 4) Merkle tree.

Block 4 of the Blockchain network has been introduced into the chain via a miner. This implies that a miner has done significant processing work by means of the Proof-of-Work prerequisite. This vilifies the authenticity of the data entered at time t1 as block B1.The IoT pump works with only one block containing prescription data. It

does not store a redundant copy of the Block thus requiring minimal memory. The feedback from the device is stored on to the Blockchain via intermediate miners. This allows the device's processing capacity sufficient to work with the computationally intensive miners.

B. The Blockchain Trust addendum

The Blockchain ledger can be designated as the middle man between a patient's insulin pump and the doctor's prognosis i.e. the doctor's prognosis recommendations regarding insulin dosages are uploaded as block in the distributed ledger [17, 18]. This makes the doctor's opinion open and concrete achieving non-repudiation for prescription. This block stands as the primary defense for any action taken in regards to the patient. Any deviation incurred will incur the health care provider / device accountable as the change insurrects the statement present in the chain. The block containing the prescription must be fed as the prime program into the pump. This ensures that the instruction is valid as the data (dosage specs) and its hash will corroborate authenticity of dosage. Blockchain will ensure data integrity and private key encryption systems will ensure identity. That is when a data is broadcasted from Blockchain the sender encrypts the data with its private key which can only be deciphered with its corresponding public key.

C. Security through liability

Liability is when a party is expected to adhere to a set of predetermined norms and a failure is met with severe ramifications. This principle is adopted onto insulin pumps. A new (counterfeit) block that deviates that violates the already received program must be verified by the pump with the block in the Blockchain.

Case Scenario 1: The liability of insulin pump system to execute dosage information from all valid blocks in the chain is established. Solution 1: New block arrival initiates the following:1) New block hash are verified for packet integrity at device level limiting processor strain. 2) Verify sender's identity via private key/ public key. 3) New block verification initiates dosage changes. 4) Manual intervention stored for redress.

Unauthorized entity attempting to violate integrity will be halted as the hash value of the block represents the collective hash of all its previous block data. Thus replicating it will require attacking the Blockchain and not just the insulin pump. The Blockchain is made secure by its immutable distributed nature rendering the device immune and safe. Additionally, since the processor of the pump is a subset of the communications component, such that, securing one results in securing the other.

Case Scenario 2: Out of context behavior can be used to trigger alerts in the system console as well as the Health- care provider. Sample Behavior and violation states for a forenoon session of a Diabetic patient employing IoT Insulin Pumps is shown by Table II. It can be inferred that whenever there is an inversion in the expected status and the ongoing status are inverted, the situation demands a system review.

Critical context arises when inversion occurs without human authorization. The dosage switches demand a dependable oversight agency to respond accordingly.

TABLE II: BEHAVIOR STATES OF IOT INSULIN PUMP

Duration	Meal- time	Insulin-Expected	Insulin-ongoing	User- Trigger	Inference
06:00 -08:00 Hrs	X	Basal BasalBolus	Basal Bolus Basal	NA Yes Violation	Nominal, Notify Alert
08:01 -09:00 Hrs	✓	Bolus Bolus	Bolus Basal	NA Violation	Nominal Alert
09:01 -12:30 Hrs	X	Basal BasalBolus	Basal Bolus Basal	NA Yes Violation	Nominal Notify Alert

Solution 2: Blockchain can be employed as a solution to this problem. Blockchain thorough its hash chain mechanism and distributed ledgers ensure immutability to data encompassed in it. This feature can be used to track the state change in the system as well as keep track of out of context behavior. The data to be stored is the state table that is shown in Table II. Instead of just triggering alerts to the care-giver a copy of the situation is uploaded onto Blockchain. This ensures that, not only was a trigger to indicate context switch occurred; there exists a permanent copy for study is maintained. Refer Figure 2 for state transition diagram. Figure 2 outlines importance of Blockchain and insulin pumps design to run perpetually. The legitimate reasons for Insulin pump to terminate functionality are 1) Battery replacement 2) Cartridge replacement 3) Patient opting removal. If the system should encounter any other situation it indicates erratic behavior that must be studied as and equivalent to anomalous behavior [19, 20]. Data access is restriced to recognized users of Blockchain. The chain may include the patient, health care provider and developer. Each of these entities may be able to respond with a long term

solution. IoT Insulin Pump(s) contain a repository of all failure cases that can only be accessed by authorized user namely patient, health care provider and developer.

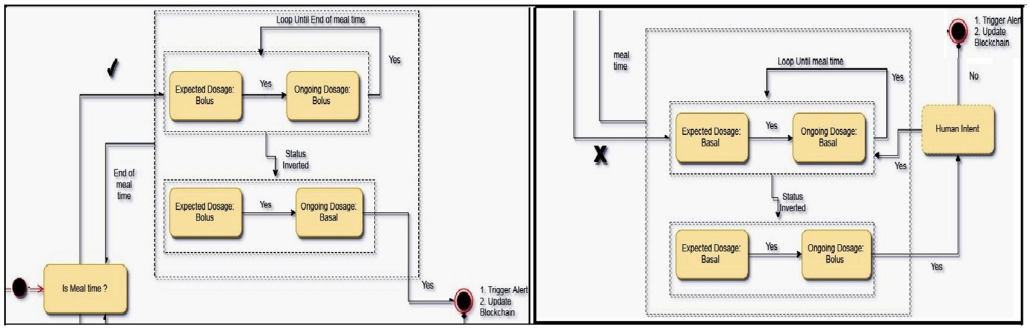

Figure 2. The State transition diagram – IoT / BC insulin Pump

V. Proof Of Impenetrability Through Propositional Calculus

In this section, causal relationship between the Insulin pump failures during operation and impaacts is outlined via Propositional calculus. Subsequently, two case scenario solutions mentioned will be modelled as mathematical relationships to observe the viability. Propositional calculus is first used to establish the indisputable facts about the system [21]. As axioms, the unchanging opposing facts are introduced one after the other. The goal is to show that systems fail when the predicted and real states are out of sync. Secondly, to introduce solution axioms that negates the contradiction introduced by opposing axioms proving the annulment of infection. Logically, the original fully functioning system can be represented as a tautology i.e. it retains "true" for all proper inputs. Opposing entities introduce protocols that fork the systems' operational parameters resulting in "contradiction" which is the mathematical equivalent of system collapse. The solution re-achieves tautology. The premise is described in table III and solutions in table IV and V.

TABLE III. PREMISE OF IOT PUMP WORKING

No.	Statement	Axiom
1.	Data in Blockchain is immutable; Basal and bolus are mutually exclusive.	BC; BS, BL && BS = !BL
2.	Two triggers normal time and mealtime that's mutually exclusive.	NT, MT && NT = !MT
3.	Normal time triggers basal dosagestate; Normal time basal dosage triggers continual loop; Meal time triggers bolus dosage.	NT → BS; BS → L; MT → BL
4.	Meal time bolus dosage triggersbasal dosage at normal time.	BL∧NT → BS
5.	User triggers bolus dosage; Outsider should not change dosage.	U → BL; !U →!BS, !U→!BL
6.	Outsider changes dosage triggersloop break, BC dataentry and system halt.	(!U→BS)→BC∧H and (!U→BL)→BC∧H
7.	Registration and halt happens only	BC ∧H ←→!L

Scenario 1: The Fully functioning system at nominal conditions will run perpetuallywith basal and bolus dosages that run on time intervals. Termination state initiates halt of the system and Blockchain entry. Axiom representation: 1) Successful State: L 2) Failure State: BC ^ H(or):L. Formal Proof: Contraposition and Without-user intervention. The absence of threat the system must running perpetually is outlined in Table IV.

TABLE IV: SYSTEM WITHOUT & WITH MALICIOUS ATTACK

WITHOUT MALICIOUS ATTACK (a)			EXTERNAL OPPOSITION (b)	
Step	Proposition	Derivation	U→ BL	Given
1.	NT→ BS, BS → L, MT, NT	Given	(!U→ BS) → BC ∧ H	Axiom (10)
2.	!BS →!NT	Contraposition (1)	!(BC∧H) →!(!U → BS)	Contraposition (4)
3.	MT=!NT , BL =!BS	Negation: axiom (3) and (2)	!(BC∧H) → (U →!BS)	Association (5)
4.	!BS→ MT	Using (6) in (5)	!(BC∧H) → (U → BL)	BS, BL (mutually exclusive)
5.	BL→ MT	Using (7) in (8)	!(!L) → (U → BL)	Axiom (11)
6.	!MT	Negation (3)	L → (U → BL) & !U→!BL	Double negation (8) & (3)
7.	!BL	Modus Tollens: (9) and (10)	!(U→ BL)	Association (10)
8.	BS	!BL=BS Axiom (2)	!L	Modus Tollens: (9) and (11)
9.	L	Conditional Proof of (5)	BC∧H ; U→ BL	Axiom (11); Given

Scenario 2: The system under attack will have mismatching states of operation & time factor. The time factor is the fundamental premise of insulin actuator. Proper detection of interference triggers the insulin dosage break and initiates entry into fault data register. The state "H" will be triggered as a result halting the system. This halt prvides safety and time to resolve device. Axiom representation: 1) Successful State: L 2) Failure State: BC ^ H(or):L. Formal Proof: Contraposition with opposing user intervention. The system is proven to halt in the presence of deviation in premise. Ref Table IV (b). Above inferences establish the Insulin pump's discrimination of a legitimate system from a corrupted system. This mutual exclusion ensures abnormal halt.

VI. Implementation Through IoT-Blockchain Prototype

An experimental prototype Fig 4 was developed using Arduino Nano IoT microprocessor and radio frequency signal generator used as IoT observer that monitor the patients continuously [24, 25]. Specifications: The processor simulates a glucose value as nominal-high-suppressed phase in a cyclic pattern. Manual activation of care-giver is a direct user input which is recorded and transmitted to the private Blockchain via Wi-Fi. The RF signal generator represents the insulin pump activation if the two-man system is in agreement. Blockchain is triggered only under abnormal activation.

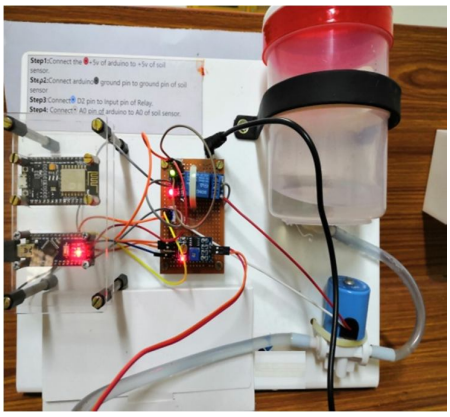

Figure 4. Prototype of IoT-Blockchain Insulin Pump

Algorithm 1_Result: Access decision incurred

```
initiation:
Decision Block Report()
time ← Block_chain_unix_clock
State ← Pump_state
dosage ← basal _ bolus
while Active do
    Activation(V NSwand, V NSstate)
    if State == active
    && time = Nominal && dosage == bolus
        then
            Nominal Activation triggered
        else
            Abnormal ActivationDetected
            /*Smart contract Incident Report∗ /
end
```

Algorithm 1: Report Generation Smart Con tract

A. Prototype Inferences

The following are the observations gained from the IoTInsulin prototype after 87 iterations of varying blood glucose from nominal < 94mmHg to high > =94mmHg. Suppressed phase need not have medical intervention. The system cannot 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 as the smart device is programmed with the seizure protocol of the patient specifically.

VII. Conclusion

The proposed system outlined two different logics that mitigated the systems' out-of-context scenarios. The first solution was a proactive system that received orders via Blockchain removing external entity penetration. The second was a reactive behavior-based solution that has binary response i.e. either it performs nominally or terminates the actuator. The Insulin Pump is highly recommended to be deployed as an IoT / Blockchain device to ensure complete overview of the patient's treatment ensuring security simultaneously. The system is a binary event-response system deisgned to eliminate prescribed failure. Future work is intended to design a live unsupervised learning algorithm with the premise of total failure removal.

References

[1] Ahamed, J., and Rajan, A. V. (2016). "Internet of Things (IoT): Application systems and security vulner- abilities". 2016 5th International Conference on Elec- tronic Devices, Systems and Applications (ICEDSA). doi: 10.1109/icedsa.2016.7818534.

[2] Pantelopoulos, A., and Bourbakis, N. G. (2010). "A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis". IEEE Transac- tions on Systems, Man, and Cybernetics, Part C. doi: 10.1109/TSMCC.2009.2032660.

[3] Hwang, D. Y., Choi, J. Y., and Kim, K.-H. (2018). “Dynamic Access Control Scheme for IoT Devices using Blockchain” International Conference on Information and Communication Technology Convergence (Ictc). S.l.: IEEE. doi: 10.1109/ICTC.2018.8539659.
[4] He, H., and Maple, C. (2016). “The security challenges in the IoT enabled cyber-physical systems and opportuni- ties for evolutionary computing and other computational intelligence”. IEEE Congress on Evolutionary Computa- tion (CEC). doi: 10.1109/CEC.2016.7743900.
[5] Harris, A. F., and Sundaram, H. (2016). “Security and Privacy in Public IoT Spaces”. 25th International Confer- ence on Computer. doi: 10.1109/ICCCN.2016.7568573.
[6] Williams, R., McMahon, E., Samtani, S., Patton, M., and Chen, H. (2017). ”Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach,” 2017 Ieee International Conference on In- telligence and Security Informatics (Isi 2017): Beijing, China, 22-24 July 2017. Piscataway, NJ: IEEE. doi: 10.1109/ISI.2017.8004904.
[7] Bouhenguel, R., Mahgoub, I., and Ilyas, M. (2008). ”Bluetooth Security in Wearable Computing Applica- tions” International Symposium on High Capacity Op- tical Networks and Enabling Technologies: (Honet) ; Penang, Malaysia, 18-20 November 2008. Piscataway, NJ: IEEE. doi: 10.1109/HONET.2008.4810232.
[8] Wireless Insulin Pump. (January 14, 2020). Retrieved from https://web.archive.org/web/ 20200430052542/https://www.nxp.com/applications/ solutions/industrial/healthcare/wireless-insulin-pump: WIRELESS-INSULIN-PUMP.
[9] Frustaci, M., Pace, P., and Aloi, G. (2017). ”Securing the IoT world: Issues and perspectives,” Ieee Conference on Standards for Communications and Networking (Cscn). IEEE / Institute of Electrical and Electronics Engineers Incorporated. doi: 10.1109/CSCN.2017.8088629.
[10] El-Azouzi, R. S., Menasche, D. D., Sabir, E. undefined, Pellegrini, F. undefined, and Benjillali, M. undefined. (2017). ”Privacy Preservation in the Internet of Things” Advances in Ubiquitous Networking 2 Proceedings of the UNet16. Singapore: Springer Singapore.
[11] Sain, M. J., Kumar, P. J., Lee, Y.-D. J., and Lee, H.J. (2010). ”Secure middleware in ubiquitous healthcare,” Iccit 2010: the 5th International Conference on Com- puter Sciences and Convergence Information Technol- ogy: November 30-December 2, 2010, Grand Hilton Ho- tel, Seoul, Korea. Piscataway, NJ: IEEE. doi: 10.1109/IC- CIT.2010.5711222.
[12] Das, A. K., Pathak, P. H., Chuah, C.-N., and Mohapatra, P. undefined. (2016). ”Uncovering Privacy Leakage in Ble Network Traffic of Wearable Fitness Trackers” Pro- ceedings of the 17th International Workshop on Mobile Computing Systems and Applications. New York, NY: ACM. doi: 10.1145/2873587.
[13] Langone, M., Setola, R., and Lopez, J. (2017). ”Cyber- security of Wearable Devices: An Experimental Analysis and a Vulnerability Assessment Method”2017 ieee 41st annual computer software and applications conference (compsac 2017). PISCATAWAY: IEEE Press Books. doi: 10.1109/COMPSAC.2017.96.
[14] Naidu, V., Mudliar, K., Naik, A., and Bhavathankar, P. (2018). ”A Fully Observable Supply Chain Management System Using Block Chain and IOT,” 3Rd International Conference for Convergence in Technology (I2CT). S.l.: IEEE. doi: 10.1109/I2CT.2018.8529725.
[15] Jeon, J. H., Kim, K.-H., and Kim, J.-H. (2018). ”Block chain based data security enhanced IoT server platform” International Conference on Information Networking (Icoin). S.l.: IEEE. doi: 10.1109/ICOIN.2018.8343262.
[16] Lee, C. H., and Kim, K.-H. (2018). ”Implementation of IoT system using block chain with authentication and data protection” International Conference on Infor- mation Networking (Icoin). S.l.: IEEE. doi: 10.1109/I-COIN.2018.8343261.
[17] Why blockchain and IoT are best friends. (January 14, 2020). Retrieved from https://web.archive.org/web/20200430052055/https://www.ibm.com/blogs/blockchain/2018/01/ why-blockchain-and-iot-are-best-friends/.
[18] Blockchain IoT Use Cases. (January 14, 2020). Retrieved from https://web.archive.org/web/20200430052404/https://www.leewayhertz.com/ blockchain-iot-use-cases-real-world-products/.
[19] Blockchain Explained. (January 14, 2020). Retrieved from https://web.archive.org/web/20200430053519/https://www.investopedia.com/terms/b/blockchain.asp.
[20] Conoscenti, M., Vetro`, A., and Martin, J. C. D. (2016). ”Blockchain for the Internet of Things: A systematic literature review” Ieee/Acs 13th International Conference of Computer Systems and Applications (Aiccsa). S.l.: IEEE. doi: 10.1109/AICCSA.2016.7945805.
[21] Propositional calculus. (n.d.). In Wikipedia. (January 14, 2020). Retrieved, from https://perma.cc/FA5M-66E7.
[22] Roy, Sandip, Chatterjee, Santanu, and Mahapatra, Gau- tam. ‘An Efficient Biometric Based Remote User Authentication Scheme for Secure Internet of Things Envi- ronment’. 1 Jan. 2018 : 1403 – 1410.
[23] Umadevi, K.S., Balakrishnan, P., and Kousalya, G. ‘Intru- sion Detection System Using Timed Automata for Cyber Physical Systems’. 1 Jan. 2019 : 4005 – 4015.
[24] Dai, H., D’angelo, L. T., & Lueth, T. (2010). Con- tinuous blood pressure monitor with wireless interface. 2010 IEEE International Conference on Robotics and Biomimetics. doi:10.1109/robio.2010.5723299
[25] Li, L., Li, Y., Yang, L., Fang, F., & Sun, Q. (2020). A Wearable Optical Fiber Wristband for Continuous and Accurate Blood Pressure Monitoring. Conference on Lasers and Electro-Optics. doi:10.1364/cleo at.2020.am3i.1