IoT Device Identity Management and Blockchain for Security and Data Integrity

Pranav Gangwani
Department of Electrical & Computer Engineering
Florida International University
Miami, Florida, USA

Santosh Joshi
Applied Research Center
Florida International University
Miami, Florida, USA

Himanshu Upadhyay
Applied Research Center
Florida International University
Miami, Florida, USA

Leonel Lagos
Applied Research Center
Florida International University
Miami, Florida, USA

ABSTRACT

Human-human or human-device communication has traditionally been the most prevalent kind of communication, however, the Internet of Things (IoT) promises to dramatically expand the Internet by enabling machine-machine (M2M) communication. The ever-increasing reliance on data to form the bases associated with decision-making processes requires data that can be trusted emanating from known devices. These devices often contain important and confidential data such as personal credentials, financial status, health data, and other private and sensitive data. Therefore, the integrity of these devices and associated data are imperative for further usage and processing. Moreover, due to the deployment and participation of a massive number of devices in the IoT ecosystem, management of identities and mitigating security vulnerabilities are two major challenges that must be addressed. The large majority of these devices are susceptible to breaches and malicious actions compromising the integrity of their data, therefore identity validation of these devices is crucial as it is a means to ensure whether data attained from these devices can be trusted. An innovative technology called blockchain has recently been developed to address several IoT security concerns and ensure the integrity of the data collected from these IoT devices. This paper proposes a technique for IoT identity management called PUF-based Device Identity Management (PUF-DIM) that employs Physical Unclonable Function (PUF) to perform device identity management to establish trust in the data associated with each device and a device's unique identifier. Moreover,a review of the major security problems with IoT and how blockchain plays a significant role in tackling those issues is discussed. Finally, a blockchain-based IoT data integrity technique is proposed for ensuring that IoT data is authentic and tamper-proof. The presented technique incorporates the consensus mechanism as well as the chain structure within the data integrity scheme for IoT.

General Terms

Identity Management, IoT Security, IoT Data Integrity

Keywords

Blockchain, IoT, Identity Management, PUF

1. INTRODUCTION

As technology is advancing, IoT is rapidly growing and forming a global network, where a vast number of devices will be connected to the internet [1]. IoT will bring endless opportunities and have an impact on every aspect of our society. The rapid growth of IoT devices has created great prospects, but at the same time has created significant concerns when it comes to sources of invalid data [2]. In general, with trillions of IoT devices, and the huge quantity of data they generate, the utmost challenge is how to uniquely identify these devices or allocate digital identities. Moreover, securing these devices from various threats and attacks and determining the integrity of the data gathered from these IoT devices are also crucial challenges that must be addressed [3]. Specifically, IoT has provided the opportunity to gather significant quantities of data enabling processes to more comprehensibly be monitored to detect anomalies [4] and effective actions to prevent failures or respond to cyberattacks.

Blockchain's underlying basis is a decentralized, distributed ledger enforced without a central authority such as an agency, bank, company, or any organization. Fundamentally, it allows a set of users to execute transactions on the distributed network in such a way that when the network is operating normally, no transaction can be altered once published. All the transactions in the blockchain are saved as a chain of blocks and this list or chain expands as new blocks are added persistently [5]. This makes blockchain an alluring technology for developers and researchers working in the IoT domain, to record and track every transaction or data sample from their respective devices.

Many IoT devices exchanges and produces a huge volume of private and critical data [6]. These IoT devices are more susceptible to attacks as compared to other endpoint devices like tablets, smartphones, or computers due to their restricted storage, processing, and network power [7]. Conventional security methods [8] tend to reveal noisy or incomplete data which may potentially impede some IoT applications and hence a proper security mechanism or process is required. Subsequently, IoT requires scalable, lightweight, and distributed solutions to achieve security and privacy protection [9]. A secure encryption technique is required to ensure data confidentiality as IoT data moves across numerous hops within a network. Blockchain technology possesses the capability to overcome the above-mentioned challenges because of its immutable, distributed, and secure nature.

Data has nowadays become a crucial asset [10], especially in the IoT domain. Data is utilized and gathered not only in the IoT systems, but in many areas such as data-driven power plants [11], health [12], transportation [13], and social media [14]. As computer-aided human functions are depending so much on data or information, trust has become a vital component. However, due to the crucial role that data plays, it has become a highly alluring target for attackers that aim to compromise the fundamental qualities that data have to exhibit to be credible, such as privacy, coherence, and accessibility [15].

To summarize, the contribution of the paper is shown below-

1) Propose a technique for IoT identity management called PUF-DIM that uses the PUF to uniquely identify each IoT device.
2) Review the major security vulnerabilities of IoT and how blockchain can address these vulnerabilities.
3) Propose a blockchain-based technique to ensure IoT data integrity.

The rest of the manuscript is organized as follows: Section 2 describes the relevant literature and the motivation for the proposed model. Section 3 explains identity management and the proposed PUF-DIM method. Section 4 discusses the security solutions offered by PUF against various threats. Section 5 discusses the technical concepts of blockchain and how it contributes to the enhancement of IoT security. Section 6 discusses the proposed blockchain-based IoT data integrity technique in detail. Section 7 discusses the conclusion of this research and future directions.

2. RELATED WORK

There is currently a plethora of researchers working on IoT device identity management, ensuring the security and data integrity of IoT devices using blockchain. However, the combined approach for PUFDIM and Physical Key Generator (PKG), combined with the proposed blockchain-based IoT data integrity makes the research contributions unique.

Horrow et al. [16] proposed an IoT identity management framework with cloud computing as its core technology. The framework used cloud technology to store and manage IoT thus, creating a centralized system. The proposed framework could efficiently authenticate and identify each IoT device. However, the proposed centralized identity management framework is software-based where the IoT devices were connected to the cloud which can function as a single point of failure.

Farid et al. [17] proposed an approach that integrated IoT and cloud computing technology to enable IoT identity management for the healthcare domain. Their proposed framework could authenticate each IoT device using encrypted biometric features. The authors used Homomorphic Encryption as the type of encryption scheme for additional security to patients' data, where the data was processed in the cloud. The proposed approach was evaluated and assessed with different users and produced 100% accuracy.

Chan Hyeok Lee et al. [18] applied "Zero-Knowledge proof" to a system of smart meters, to protect IoT data and to prove that the information is true without disclosing details to the verifier. This research prevented two major security threats such as data counterfeiting and data tampering to smart metersby introducing and applying blockchain technology. The authors proposed a system environment that shared IoT data from devices to the application by employing the Mobius IoT open server platform. Once the data was shared, this platform, uploaded that data to a blockchain server. Additionally, the authors integrated their blockchain implementation along with "Zero-knowledge proof" to prevent disclosing confidential data such as account information.

Yang et al. [19] presented a method that used deep learning algorithms to produce unique fingerprints for IoT devices. The authors found the device features by observing the differences in software implementations from different manufacturers and analyzing 20 IoT protocols. A prototype was built to implement and evaluate the proposed fingerprinting approach. After experimental evaluation, the device classification results produced 94.7% precision and 95% recall.

Yousefnezhad et al. [20] proposed an IoT identity management method that uses machine learning classification algorithms. For performing identity management, statistical features, sensor values, and header information was obtained by monitoring the network packets arriving from IoT devices. Once the data was obtained, the authors applied machine models to uniquely identify each IoT device on the network. However, the authors' approach was highly dependent on the data and centralized which could become a single point of failure.

All the described relevant literature for IoT identity management were either software-based methods that were highly dependent on data or centralized approaches which could become a single point of failure. However, the proposed identity management approach uses PUF to uniquely identify IoT devices and establish trust. To ensure the integrity and security of IoT data in a distributed and decentralized way, this research integrates blockchain technology with PUF.

3. IDENTITY MANAGEMENT

The administration of individual identities within a system is depicted by identity management. There is no deterrence or accountability without unforgeable, unique, and easily verifiable identities. In the world of IoT, the identity management system must be able to identify sensors, devices, monitors, etc., and also their access to data that can be both sensitive and non-sensitive [21].

3.1 PUF-based Device Identity Management (PUF-DIM)

This research focuses on the IoT devices' physical properties andcommunications and how to use them for the authentication of devices. These IoT devices utilize a range of protocols forcommunication and the proposed method relies on utilizing both the Physical Key Generation (PKG) as well as the Physical Unclonable Function (PUF). The proposed identity management method enhances the security of IoT devices by integrating PKG with PUF. The authentication process occurs in four mainstages and is shown in Fig. 1. First is the Enrollment Stage; during this stage, the manufacturer creates a series of challenges at random and presents them to the PUF. Each challenge is responded to with a response R by the PUF. In the second stage, the device's secret key is generated by a function W. This stage is stated as the "Key Generation Stage" and is continued by the PKG which produces the key, K_i from the noisy channel of the PUF which is then utilized as the symmetric encryption key. The third stage, also known as the "Authentication Stage," operates by hashing the key K_i, obtained from the previous stage which is then utilized to retrieve a challenge with a recognized response. Given that the PUF is aware of all valid challenges, the PUF produces a response R_i by utilizing the helper Data function W. The server which is encrypted by K_i receives the hash of the response$H(R_i)$. The final stage is also known as the Re-Enrollment Stage. Once a secure connection between the server and the device is set up, this stage is executed. In this stage, a new set of responses that are authorized, helper data, and challenges are all replenished [22].

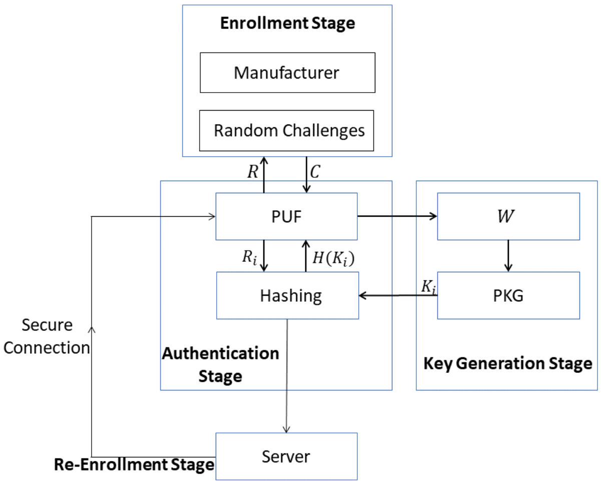

Fig 1: Proposed Authentication Method using PUF

Fig. 2 depicts the proposed method for IoT authentication using PUF. This method assumes that a PUF can possess innumerable Challenge-Response-Pairs (CRPs). For each challenge and each Integrated Circuit (IC), the PUF response is unique. Another important point to consider is the difficulty in achieving model building for a given PUF due to the non-linearities present in it. When an authentic IC is in charge of a trustworthy environment, it employs randomly selected challenges to achieve unanticipated results. To perform future authentication checks and collect the PUF response from the IC, these CRPs are stored by a reliable and trustworthy entity. To demonstrate that the IC is legitimate, the response must match with or be sufficiently similar to the previously recorded response. Since only the trusted party and IC should be aware of the CRP. To prevent Man-in-the-middle attacks, these challenges are never repeated. As a result, responses and challenges can be sent throughout the authentication process in plain text [23].

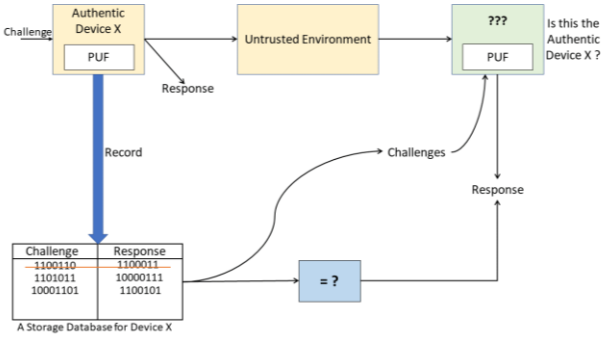

Fig 2: System Overview

4. THREATS AND SECURITY SOLUTIONS OF PUFS

In this section, various possible vulnerabilities to the proposed PUF-DIM approach is discussed and how the PUF provides security against it.

4.1 Obtaining the K_i through Eavesdropping

The same communication channel must be heard by an eavesdropping attacker in order to procure the key K_i and enough information must be obtained from the reconciliation step to obtain the key K_i from the eavesdropper's channel [24]. However, due to the properties of PKG, it is not possible to eavesdrop on the same channel. Moreover, sufficient information (e.g., parity bits) cannot be eavesdropped on by an attacker in the reconciliation step to build the key K_i[25].

4.2 Impersonating a New Device

It is possible to validate whether a PKG-negotiated key genuinely belongs to an intended device by using the unclonable property of PUFs. Due to the strong authentication features of the PUF, Man-in-the-Middle attacks cannot occur in the network [26]. Also, due to this an attacker is not able to join the network with a counterfeit device. Stronger security requirements can be attained with the help of tamper resistant PUFs (for instance coating PUFs).

4.3 Impersonating a Device after the Key Generation Stage Knowing the Manufacturer's CRP Database

An attacker can attain the CRPs that are valid, from the server of the manufacturer because of an intrusion attack or leakage of data. For the Authentication Stage [27], it is still not enough to own a valid and justifiable response R. The shared secret key which is generated by PKG is utilized in order to derive the challenge C. This key is not transmitted and is calculated separately on the IoT device. Therefore, the shared key K_i should be eavesdropped on by an attacker or must estimate the correct response (sent encrypted with K_i) with a calculated probability.

4.4 Compromising the Network by Compromising a Device

An attacker cannot obtain previously deployed keys if the IoT device is compromised [28]. A new, truly random shared secret key K_i is produced by PKG over a wireless channel for each pair of devices which provides an opportunity for re-keying. Hence, if only one device is compromised, it yields the key to that specific device while the other generated keys remain safe.

4.5 Waiting for User Error

A user might make a mistake while an attacker could wait for that mistake to occur. However, minimal user interaction is achieved with the combination of PUFs and PKG.

For instance, there are high chances that a user could make a few mistakes while turning a sensor mode on. All the security and key establishment measures automatically take place and emphasize usable security. The sensor nodes will not operate correctly in the event of an error; therefore, the combined procedure must be started again. To accurately identify the nodes, their LED display results can be used (red LED: unsuccessful installation, green LED: successful installation) [29].

5. IoT SECURITY USING BLOCKCHAIN

A blockchain [30] is a distributed ledger or a distributed and immutable database that operates in a decentralized and peer-to-peer network (P2P). The data within the blockchain is constituted in blocks that are linked cryptographically. These blocks of data are validated by miners who perform mining and are timestamped. The blockchain utilizes the SHA-256 hashing algorithm along with Elliptic Curve Cryptography (ECC) to make the entire data structure immutable and authentic [31]. Moreover, every block in the blockchain is linked to the previous block by constituting a 256-bit hash of the previous block. These blocks also contain a list of transactions which is verified by the miners. The miner nodes are special nodes in the blockchain that is responsible for verifying and validating the transactions and the blocks in the blockchain [32].

The block-based structure of the blockchain is shown in Fig. 3. Each block in the figure contains two major components, the block header and the block body which comprises the transaction list. Whereas the block header constitutes fixed and variable fields such as version number, block size, nonce, timestamp, difficulty, and the block header hash. To keep a track of the blockchain protocol upgrades, the block version number is used. There is another field within the block header, called Merkle root [33] which is a root hash value obtained by hashing all the transactions in the block body. A nonce is a variable field inside the block header that the miners use for mining and finding the correct value of the nonce is the goal of the miners.

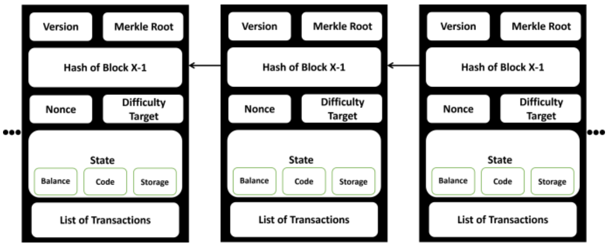

Fig 3: Design Structure of Blockchain

5.1 Blockchain Solutions

This section summarizes and discusses various blockchain features [34] that can contribute to the security of IoT devices and data.

5.1.1 Space for Address

160-bit is the address allocation for blockchain in contrast to the address space of IPv6 which is 128-bit. The “Elliptic Curve Digital Signature Algorithm (ECDSA)” generates a public key of 20 bytes, and a 160-bit hash of that public key is allocated as the blockchain's address space [35]. With the 160-bit address, blockchain can assign and generate addresses offline for about 1.46 * 10^{48} IoT devices. The approximate probability is 10^{-48} for address collision which is secure to present a Global Unique Identifier (GUID). While allocating and assigning an address to an IoT device, GUID does not require any unique registration or verification.

5.1.2 Integrity and Authentication of Data

Due to the blockchain’s design structure [36], IoT data, when stored on the blockchain will be immutable due to cryptographic linkages. To authenticate and ensure the integrity of the transmitted data, the sender adds a unique signature by using the GUID and a public key [37]. Additionally, all the transactions executed by the IoT devices on the blockchain can be safely and securely tracked, thus, providing an authentic audit trail.

5.1.3 Governance and Identity of Things (IDoT)

Several challenging issues must be addressed for IoT by “Identity and Access Management (IAM)” in a reliable, trustworthy, and efficient way. A major problem is dealing with identity relationships and ownership of IoT devices. If a device gets resold, decommissioned, or compromised, consumer ownership can be changed or revoked. Another challenge is the handling of relationships and attributes of an IoT device. For example, serial number, manufacturer, type, make, and location are some of the attributes. These challenges can be securely, easily, and efficiently solved by using blockchain. Providing ownership tracking, authorized and trustworthy identity registration, and monitoring of assets, products, and goods are the main factors for which blockchain has been used broadly. In order to enable trusted transactions in a distributed environment and simultaneously maintain the integrity of the transactions, various approaches, for example, TrustChain [38] are proposed with the help of using blockchain. TrustChain registered and identified the IoT devices which were connected to the blockchain and stored the data about their complex relationships on the blockchain.

5.1.4 Authentication, Authorization and Privacy

Smart contracts running on the blockchain can authenticate IoT devices [39] due to the logic that defines smart contracts and the authentication rules within them. As compared to the conventional authorization protocols such as “OAuth 2.0,” “Role Based Access Management (RBAC),” “LWM2M”, and “OpenID”, smart contracts can enable IoT device access control policies more simply. Additionally, smart contracts provide data privacy and specify who can upgrade, update, patch the IoT hardware or software, provide new key pairs, reset the IoT device, change ownership and initiate a service or repair request.

5.1.5 Secure Communications

The IoT protocols associated with routing as those of 6LoWPAN and RPL and even the application protocols such as MQTT, HTTP, or XMPP [40] are not secure by design. To secure the messaging and communication of these protocols, they are overlapped by other security protocols such as TLS and/or DTLS. Similarly, to provide security for 6LoWPAN and RPL, IPSec for routing is typically used. IPSec, TLS, DTLS, and also the lightweight “TinyTLS” protocols require high memory and computation. They are also complicated in terms of governance, centralized management of keys, and distribution using the popular PKI protocol. In the blockchain, distribution and key management are completely disregarded. Since every IoT device would have its asymmetric key pair and unique GUID after the installation is done and is connected to the network of blockchain [41].

6. PROPOSED BLOCKCHAIN-BASED IoT DATA INTEGRITY TECHNIQUE

This section explains the main reason behind the convergence of blockchain technology and IoT. Every node in the blockchain network must contribute to the consensus mechanism, however, this becomes a major challenge for the IoT device nodes as they are limited in memory and power [42]. A major assumption of the proposed blockchain-based technique is that the total number of nodes is the same as that of the cooperative nodes in the existing blockchain network. Thus, if an adversary is successfully able to control more than 50% of the nodes, the entire blockchain network will be compromised. However, the proposed blockchain-based IoT data integrity technique overcomes this vulnerability and prevents these types of attacks by introducing a level of uncertainty of various node combinations.

The current blockchain is enhanced with the following additional techniques-

1) Random Selection of CooperativeNodes: In the suggested technique, the randomly selected cooperative nodes rebroadcast the shared IoT data. Additionally, solving the cryptographic puzzle to attain consensus like the existing blockchain is not required by each node.

2) Majority-based Verification: Only the majority of the received data will be evaluated by each node. The computation overhead of the IoT nodes can be reduced in the current blockchain by preventing the encryption and decryption process required by digital signatures.

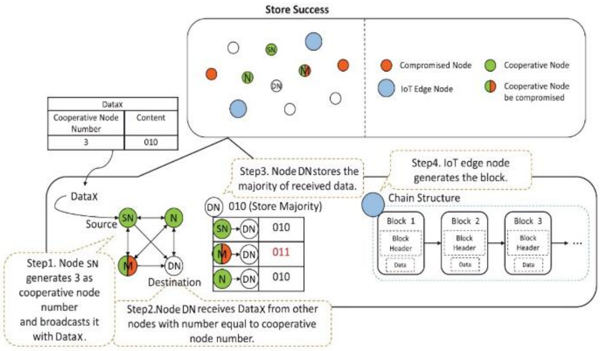
Store Success
Compromised Node
Cooperative Node
IoT Edge Node
Cooperative Node be compromised
SN
N
M
DN
DataX
Cooperative Node Number
Content
3
010
DataX
Source
Destination
Step1. Node SN generates 3 as cooperative node number and broadcasts it with DataX.
Step2.Node DN receives DataX from other nodes with number equal to cooperative node number.
Step3. Node DNstores the majority of received data.
010 (Store Majority)
010
011
010
Step4. IoT edge node generates the block.
Chain Structure
Block 1
Block 2
Block 3
Block Header
Data
...

Fig 4: Proposed Blockchain-based IoT Data Integrity Technique

6.1.1 System Description

In the proposed technique, first, several cooperative nodes Y is randomly produced by the source node SN. The source data that includes this number will be broadcast to the network. Each node then rebroadcasts the information while receiving the source information. Once the received data matches the cooperative node number, the rebroadcasting process will stop. The cooperative node is also referred to as the source node in the proposed technique. The other cooperative nodes are selected according to the reception sequence in the destination node. The subsequent unknown aspects affect the reception sequence-

- The transmission time needed by the source node to receive the data
- The time of waiting for the data in the nodes

The above aspects are linked to the present status of the network, like packet collision rate and channel quality.

Fig. 4 elucidates the proposed technique, where the source data is denoted as "010" also known as "Data X" along with three cooperative nodes. Essentially, the proposed blockchain-based IoT data integrity technique occurs in four main stages. In the first step, the source node SN generates the cooperative node number as 3 and then broadcasts it to the network along with "Data X". Let nodes M and N be the first and second ones to rebroadcast the source data from SN. Therefore, M and N are the cooperative nodes. In step 2, the destination node DN receives Data X from other nodes where the cooperative node number is 3. After receiving three "Data X" from the node SN, M, and N, all the other nodes will stop rebroadcasting "Data X." Step 3 includes the storage of the majority of the received data by the destination node DN. Finally, in step 4, the block for the blockchain is generated by the IoT edge nodes as shown. All the blockchain nodes, after comparing the received "Data X," store the majority of it. As shown in Fig. 4, the "Data X" can be directly stored on the destination node DN even after only one cooperative node gets compromised. Using its stored data, each node will verify the received block [43].

7. CONCLUSION AND FUTURE WORK

Nowadays threats to IoT devices are continuously increasing at an alarming rate. This is mainly because of the restricted resources in these devices, the deficiency of software design, and secure hardware. This research paper identifies the IoT devices by their unique identification number by employing device identity management using PUFs and PKG. A detailed survey about the security problems and risks related to the IoT domain is performed in this research and how blockchain could solve these issues. Finally,this paper proposes a blockchain-based technique to ensure that the data collected from the IoT devices is authentic and tamper-proof.

For the future work, a framework will be created that implements the four main aspects i.e., IoT Device identity management using PUFs, applying blockchain technology to secure those devices against various threats, implementing the proposed blockchain-based technique to showcase that the data transmitting from the IoT devices is authentic and tamper-proof if stored on the blockchain. Next, machine learning/deep learning models will be applied for anomaly detection on the data gathered by these IoT devices to check whether the data or the devicesare malicious or benign.

8. REFERENCES

[1] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," *Proc. - 10th Int. Conf. Front. Inf. Technol. FIT 2012*, pp. 257–260, 2012, doi: 10.1109/FIT.2012.53.

[2] G. S. Thejas *et al.*, "A Multi-time-scale Time Series Analysis for Click Fraud Forecasting using Binary Labeled Imbalanced Dataset," in *2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*, Dec. 2019, pp. 1–8, doi: 10.1109/CSITSS47250.2019.9031036.

[3] N. V. Dharwadkar, A. A. Dixit, A. K. Kannur, M. A. B. Kadampur, and S. Joshi, "Identification of Reasons Behind Infant Crying Using Acoustic Signal Processing and Deep Neural Network for Neonatal Intensive Care Unit," *Int. J. Inf. Retr. Res.*, vol. 12, no. 1, pp. 1–17, Jan. 2022, doi: 10.4018/IJIRR.289576.

[4] S. K. Peddoju, H. Upadhyay, J. Soni, and N. Prabakar, "Natural language processing based anomalous system call sequences detection with virtual memory introspection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 5, pp. 455–460, 2020, doi: 10.14569/IJACSA.2020.0110559.

[5] X. Zhu and Y. Badr, "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions," *Sensors (Basel).*, vol. 18, no. 12, pp. 1–18, 2018, doi: 10.3390/s18124215.

[6] S. Joshi, H. Upadhyay, and L. Lagos, "Deactivation and decommissioning web log analysis using big data technology - 15710," 2015, [Online]. Available: https://www.osti.gov/biblio/22824525.

[7] A. Tambe *et al.*, "Detection of Threats to IoT Devices using Scalable VPN-forwarded Honeypots," in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, Mar. 2019, pp. 85–96, doi: 10.1145/3292006.3300024.

[8] S. Tufail, S. Batool, and A. I. Sarwat, "A Comparative Study Of Binary Class Logistic Regression and Shallow Neural Network For DDoS Attack Prediction," in *SoutheastCon 2022*, Mar. 2022, pp. 310–315, doi: 10.1109/SoutheastCon48659.2022.9764108.

[9] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, "A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid," *Energies*, vol. 14, no. 18, p. 5894, Sep. 2021, doi: 10.3390/en14185894.

[10] H. Upadhyay, L. Lagos, S. Joshi, and A. Abrahao, "Big Data Framework with Machine Learning for D and D Applications - 19108," 2019, [Online]. Available: https://www.osti.gov/biblio/23002927.

[11] P. Gangwani, J. Soni, H. Upadhyay, and S. Joshi, "A Deep Learning Approach for Modeling of Geothermal Energy Prediction," *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, no. 1, pp. 62–65, 2020.

[12] D. Gangwani, Q. Liang, S. Wang, and X. Zhu, "An Empirical Study of Deep Learning Frameworks for Melanoma Cancer Detection using Transfer Learning and Data Augmentation," in *2021 IEEE International Conference on Big Knowledge (ICBK)*, Dec. 2021, pp. 38–45, doi: 10.1109/ICKG52313.2021.00015.

[13] D. Gangwani and P. Gangwani, "Applications of Machine Learning and Artificial Intelligence in Intelligent Transportation System: A Review," in *Choudhary, A., Agrawal, A.P., Logeswaran, R., Unhelkar, B. (eds) Applications of Artificial Intelligence and Machine Learning. Lecture Notes in Electrical Engineering*, 2021, pp. 203–216.

[14] J. Soni, N. Prabakar, and H. Upadhyay, "Towards Detecting Fake Spammers Groups in Social Media: An Unsupervised Deep Learning Approach," in *Deep Learning for Social Media Data Analytics*, T.-P. Hong, L. Serrano-Estrada, A. Saxena, and A. Biswas, Eds. Cham: Springer International Publishing, 2022, pp. 237–253.

[15] N. V. Dharwadkar, G. G. Shingan, S. U. Mane, and S. Joshi, "Enhanced Parallel-Particle Swarm Optimization (EP-PSO) Approach for Solving Nurse Rostering Problem," *Int. J. Swarm Intell. Res.*, vol. 13, no. 1, pp. 1–17, Jan. 2022, doi: 10.4018/IJSIR.298261.

[16] S. Horrow and A. Sardana, "Identity management framework for cloud based internet of things," *ACM Int. Conf. Proceeding Ser.*, pp. 200–203, 2012, doi: 10.1145/2490428.2490456.

[17] F. Farid, M. Elkhodr, F. Sabrina, F. Ahamed, and E. Gide, "A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services," *Sensors*, vol. 21, no. 2, 2021, doi: 10.3390/s21020552.

[18] C. H. Lee and K. H. Kim, "Implementation of IoT system using block chain with authentication and data protection," *Int. Conf. Inf. Netw.*, vol. 2018-Janua, pp. 936–940, 2018, doi: 10.1109/ICOIN.2018.8343261.

[19] K. Yang, Q. Li, and L. Sun, "Towards automatic fingerprinting of IoT devices in the cyberspace," *Comput. Networks*, vol. 148, pp. 318–327, Jan. 2019, doi: 10.1016/j.comnet.2018.11.013.

[20] N. Yousefnezhad, A. Malhi, and K. Främling, "Automated IoT Device Identification Based on Full Packet Information Using Real-Time Network Traffic," *Sensors*, vol. 21, no. 8, p. 2660, Apr. 2021, doi: 10.3390/s21082660.

[21] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of internet of things," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 61–65, 2013, doi: 10.1145/2517968.2517976.

[22] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the internet of things," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1305, pp. 15–20, 2017, doi: 10.1145/3102304.3102312.

[23] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *Proc. - Des. Autom. Conf.*, pp. 9–14, 2007, doi: 10.1109/DAC.2007.375043.

[24] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8205–8228, Jun. 2022, doi: 10.1109/JIOT.2022.3142084.

[25] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, pp. 128–139, 2008, doi: 10.1145/1409944.1409960.

[26] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science (80-.).*, vol. 297, no. 5589, pp. 2026–2030, 2002, doi: 10.1126/science.1074376.

[27] M. Ebrahimabadi, M. Younis, and N. Karimi, "A PUF-Based Modeling-Attack Resilient Authentication Protocol for IoT Devices," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3684–3703, Mar. 2022, doi: 10.1109/JIOT.2021.3098496.

[28] S. Joshi, H. Upadhyay, L. Lagos, N. S. Akkipeddi, and V. Guerra, "Machine Learning Approach for Malware Detection Using Random Forest Classifier on Process List Data Structure," in *Proceedings of the 2nd International Conference on Information System and Data Mining - ICISDM '18*, 2018, pp. 98–102, doi: 10.1145/3206098.3206113.

[29] C. Huth, J. Zibuschka, P. Duplys, and T. Güneysu, "Securing systems on the Internet of Things via physical properties of devices and communications," *9th Annu. IEEE Int. Syst. Conf. SysCon 2015 - Proc.*, pp. 8–13, 2015, doi: 10.1109/SYSCON.2015.7116721.

[30] P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi, and L. Lagos, "Securing Environmental IoT Data Using Masked Authentication Messaging Protocol in a DAG-Based Blockchain: IOTA Tangle," *Futur. Internet*, vol. 13, no. 12, p. 312, Dec. 2021, doi: 10.3390/fi13120312.

[31] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc., 2014.

[32] P. S. Kumar and S. Pranavi, "Performance analysis of machine learning algorithms on diabetes dataset using big data analytics," *2017 Int. Conf. Infocom Technol. Unmanned Syst. Trends Futur. Dir. ICTUS 2017,* vol. 2018-Janua, no. Iddm, pp. 508–513, 2018, doi: 10.1109/ICTUS.2017.8286062.

[33] S. Aruna, M. Maheswari, and A. Saranya, "Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root," *IOP Conf. Ser. Mater.*

Sci. Eng., vol. 993, no. 1, p. 012103, Dec. 2020, doi: 10.1088/1757-899X/993/1/012103.

[34] S. Namasudra and P. Sharma, "Achieving a Decentralized and Secure Cab Sharing System Using Blockchain Technology," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–10, 2022, doi: 10.1109/TITS.2022.3186361.

[35] A. Sultan, M. A. Mushtaq, and M. Abubakar, "IOT Security Issues Via Blockchain," in *Proceedings of the 2019 International Conference on Blockchain Technology*, Mar. 2019, pp. 60–65, doi: 10.1145/3320154.3320163.

[36] S. Namasudra, P. Sharma, R. G. Crespo, and V. Shanmuganathan, "Blockchain-Based Medical Certificate Generation and Verification for IoT-based Healthcare Systems," *IEEE Consum. Electron. Mag.*, pp. 1–1, 2022, doi: 10.1109/MCE.2021.3140048.

[37] A. R. Reddy and P. S. Kumar, "Predictive big data analytics in healthcare," *Proc. - 2016 2nd Int. Conf. Comput. Intell. Commun. Technol. CICT 2016*, pp. 623–626, 2016, doi: 10.1109/CICT.2016.129.

[38] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 770–780, 2020, doi: 10.1016/j.future.2017.08.048.

[39] P. Sharma, N. R. Moparthi, S. Namasudra, V. Shanmuganathan, and C. Hsu, "Blockchain- based IoT architecture to secure healthcare system using identity- based encryption," *Expert Syst.*, Dec. 2021, doi: 10.1111/exsy.12915.

[40] A. O. Bang, U. P. Rao, A. Visconti, A. Brighente, and M. Conti, "An IoT Inventory Before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research Directions," *Comput. Secur.*, vol. 123, p. 102914, Dec. 2022, doi: 10.1016/j.cose.2022.102914.

[41] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[42] C. Decker, C. Decker, and R. Wattenhofer, "Information propagation in the Bitcoin network Information Propagation in the Bitcoin Network," *13-th IEEE Int. Conf. Peer-to-Peer Comput.*, no. August, pp. 1–10, 2016, doi: 10.1109/P2P.2013.6688704.

[43] Y. J. Chen, L. C. Wang, and S. Wang, "Stochastic Blockchain for IoT Data Integrity," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 373–384, 2020, doi: 10.1109/TNSE.2018.2887236.