Measurement: Sensors 24 (2022) 100490

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Self secured model for cloud based IOT systems

G Soniya Priyatharsini [a,*], A. Jyothi Babu [b], M. Gnana Kiran [c], Sathish Kumar P.J. [d], Nelson Kennedy Babu C. [e], Aleem Ali [f]

[a] Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Chennai, Tamil Nadu, 600095, India
[b] Department of MCA, Sree Vidyanikethan Engineering College, Tirupati, Andhra Pradesh, India
[c] Department of Engineering Physics, K L University, Vaddeswaram, Andhra Pradesh, 522302, India
[d] Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, 600123, India
[e] Department of Computer Science and Engineering, SIMATS School of Engineering, SIMATS, Chennai, Tamilnadu, India
[f] Department of Computer Science &Engineering, UIE, Chandigarh University,Mohali, Punjab, India

ARTICLE INFO

Keywords:
IoT
Cloud add value services
Federated cloud
Hardware and software products

ABSTRACT

A difficult problem to solve concerns the secure installation and startup of devices connected to the Internet of Things (IoT) via the Internet.To provide additional value-added services, this article deals with the verified configuration of IoT devices in a secure manner using the Internet. Following a review of the safe self-configuration limitations imposed on IoT and Cloud technologies; offer a Cloud-based architecture that enables the communication between IoT devices and several federated Cloud services. Specifically discuss two situations, one cloud environment and federated cloud infrastructure interact with IoT devices, and handle unique issues.In addition, it provides many operational design features that take into account the truly open hardware and software products already on the market.

1. Introduction

IoT was currently used in many fields of application, including construction processes, vehicle traffic control, ecosystem analysis, medicine, weather forecasting, and video surveillance, among others [1,2].Without a doubt, there is no limit to the range of possibilities that could be realized through the merger of IoT and cloud technologies. Researchers believe that the IoT could be seen as a logical extension of cloud computing, allowing us to govern smart ubiquitous settings by accessing IoT-based resources and competencies via the network [3–5]. In addition, Internet computing can assist in the provision of IoT services.So, a cloud-based detection & actuator is a service that should be available on demand as an IoT product [6].The safe self-image of these gadgets, which would be necessary to link them to the Internet, should be one of the main problems with IoT device deployment [7].

The generation of IoT-compatible objects and the exchange of connectivity on IoT concepts and systems are important next steps in the evolution of the Internet. On the foundation of the ZigBee network, contemporary IoT solutions are being discussed [8]. An architecture based on a trusted center, which should be responsible for the management of security issues, and defines the security of sensor nodes [9]. The Internet of Things (IoT) is a massive phenomenon in which many nodes of sensors and low-power devices are linked to data bridges.This change was not simple at this time, making IoT extremely complicated [10].To avoid diluting IoT's core goals, electricity options for millions of units should be cost-effective, as IPv6 usage continues to spread worldwide.Therefore, it is necessary to standardize the common set of standards for communication systems used for IoT elements [11].The area of security faces unique challenges.As we cross the IoT area of IPv6 publishing and the Future Internet area, one of the perceptions of the global threat was on the rise [12].People increasingly want to be able to get any gadget on the web that suits their preferences and interests [13]. The IoT security space now has to respond to new concerns due to increased access to resources and skills.

Combining IoT and cloud computing opens up a wide range of potential applications, and many frameworks have been introduced to date [14].Researchers believe that IoT could look like a logical extension of cloud computing, allowing us to control ubiquitous smart settings by accessing IoT-based resources and capabilities. Additionally, cloud computing can help with IoT service delivery [15]. Consequently, an on-demand detection and activation service was an IoT service type [16].The self-configuration of IoT devices, which was required for their

* Corresponding author.
E-mail address: soniya.cse@drmgrdu.ac.in (G.S. Priyatharsini).

https://doi.org/10.1016/j.measen.2022.100490
Received 10 August 2022; Received in revised form 19 September 2022; Accepted 26 September 2022
Available online 8 October 2022

interconnection over the Internet, should be one of the major issues with deployment [17].In concept, an IoT system should be able to set itself up to communicate securely with the Cloud and should automatically adapt its behavior by acquiring required elements from the Internet [18].

2. Related works

Systems should have secret keys, encryption methods, or hidden identifiers to allow IoT systems to securely self-identify and maintain communication in the cloud [19].That strategy is already being employed. Due to the high level of interest among academic institutions and commercial enterprises in this application sector, these examples merely "reflect a few droplets in the ocean of IoT and Cloud technology." We specifically proposed a safe setup and boot process for embedded systems [20]. Two hypothetical scenarios—a Single-Cloud ecosystem and a replicated Cloud environment communicating with IoT devices—explore how to use our method in real situations in this article. Furthermore, they explore working with real open hardware and software solutions that are already on the market because they feature many design highlights.IoT companies that consider cloud computing as strategically important for the promotion of their products are the target audience for the solution described here [21].

Although this is a hotly debated issue, security in IoT and cloud computing does not impact the rapid and widespread acceptance and implementation of these systems.The author discusses the security problems and difficulties of IoT-based smart grids and describes the main security agencies that must be taken into account when managing SG protection [22].A method for rapid scanning of several IoT objects simultaneously has been given. The researchers describe the concept of Probability Yoking Proofs and three key performance evaluation standards: cost, safety, & fairness.The approach, where the researchers carry out a rigorous verification of security systems [23], integrates the message structure of traditional clustering proof constructions with an adaptive Poisson sampling technique where the likelihood that each item is examined changes over time.

RFID implant hardware has been introduced with a secure authentication mechanism.The researchers propose a system that uses lightweight D-Quark hashing and elliptical encryption. The D-Quark lightweight hash architecture takes into account costs and performance while being optimized for pervasive devices with limited resources [24]. The proposed system involves overhead communications costs that are expected to be 48% lower than current comparable methodologies, based on analytical performance monitoring.The researchers suggest a secure, flexible but reliable IoT storage framework that manages scalability, adaptability, or reliability through the information and system stages.It is based on a changed secret sharing method.Shamir's secret sharing method would be used to secure data without the heavy key exchange required by traditional cryptographic techniques.The initial

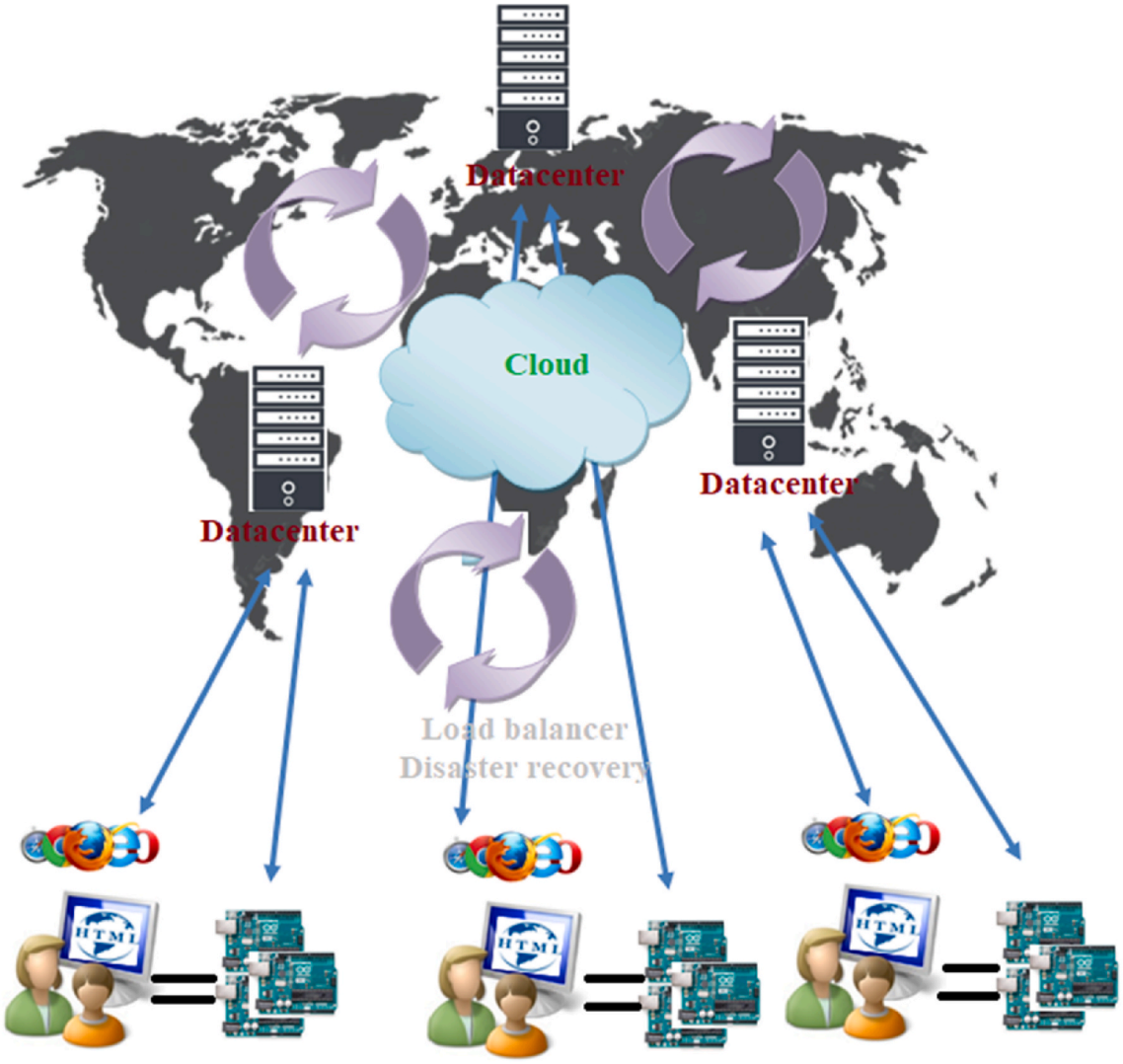

Fig. 1. Single-Cloud circumstance.

secret sharing plan has been updated to make use of all the polynomial variables to increase data storage at the database level.

3. Proposed system

Referring to Figs. 1 and 2, exhibit two difficult scenarios that designate as "Single-Cloud" & "Multicloud." In both cases, many consumers are carrying a variety of Internet-connected IoT implanted gadgets.An asset can integrate automatically by getting its configuration from a certain cloud provider [25].In the single cloud scenario, as illustrated in Fig. 1, a cloud operator's data center was dispersed around the world.For instance, data center A should be located in the United States, data center B in Europe, and data center C in Asia.A data center gathers information on IoT embedded systems linked in the service area. Since data centers are the property of various collaborating cloud services, the Multicloud situation shown in Fig. 2 is much more difficult than the previous one.

In this image, Cloud B would be an IoT network operator while Clouds A and C were device manufacturers.A federation link should be established between clouds A, B, and C to improve their business activities.The way of creating relationships between these clouds would be an intriguing subject.In addition to offering a variety of services to clients, Cloud B may also work with Clouds A and C, which offer IoT technologies.Cloud B may also be the third-party organization responsible for confirming the reliability and quality of its IoT devices.Since manufacturers have installed motherboards with trusted platform components, a similar scenario already exists in Trusted Computing. Initially, clouds A and B choose to use a single authentication service.IoT embedded devices must authenticate on Cloud B before accessing Cloud A. Upon successful verification, Cloud A will have faith in Cloud B. As a result, Cloud A will complete your device registration.Subsequently, a federating relationship is established between clouds A and B. To achieve this, Cloud B keeps track of each IoT embedded device's firmware version, bug reporting, and other details, enabling it to authenticate a device without being aware of either its owner or its actual location. Cloud B can alert Cloud A. Without sharing user data or device media access control addresses, Cloud B needs to recognize the device.

4. Secure self-identification of IoT devices

Arduino's open hardware infrastructure was a well-rounded design that can meet IoT requirements, in particular, because of its low cost & ease of use.The Arduino platform has many versions, shields, and modifications available on the market.This might offer both Linux onboard features and Arduino features is the Arduino platform.It provides a strongly connected computer with the simplicity of an Arduino and supports Linino, a Linux distribution based on OpenWRT.The Arduino component was visible to the left of the image, whereas the Linino component was visible to the right.Yun has integrated Wi-Fi and Ethernet circuits for connection.Linino could be used in our situations to implement security mechanisms and carry out internet connections.For secure communication with other devices and the cloud, it is very easy to develop on this Web client device, XMPP client, Python, or OpenSSL.

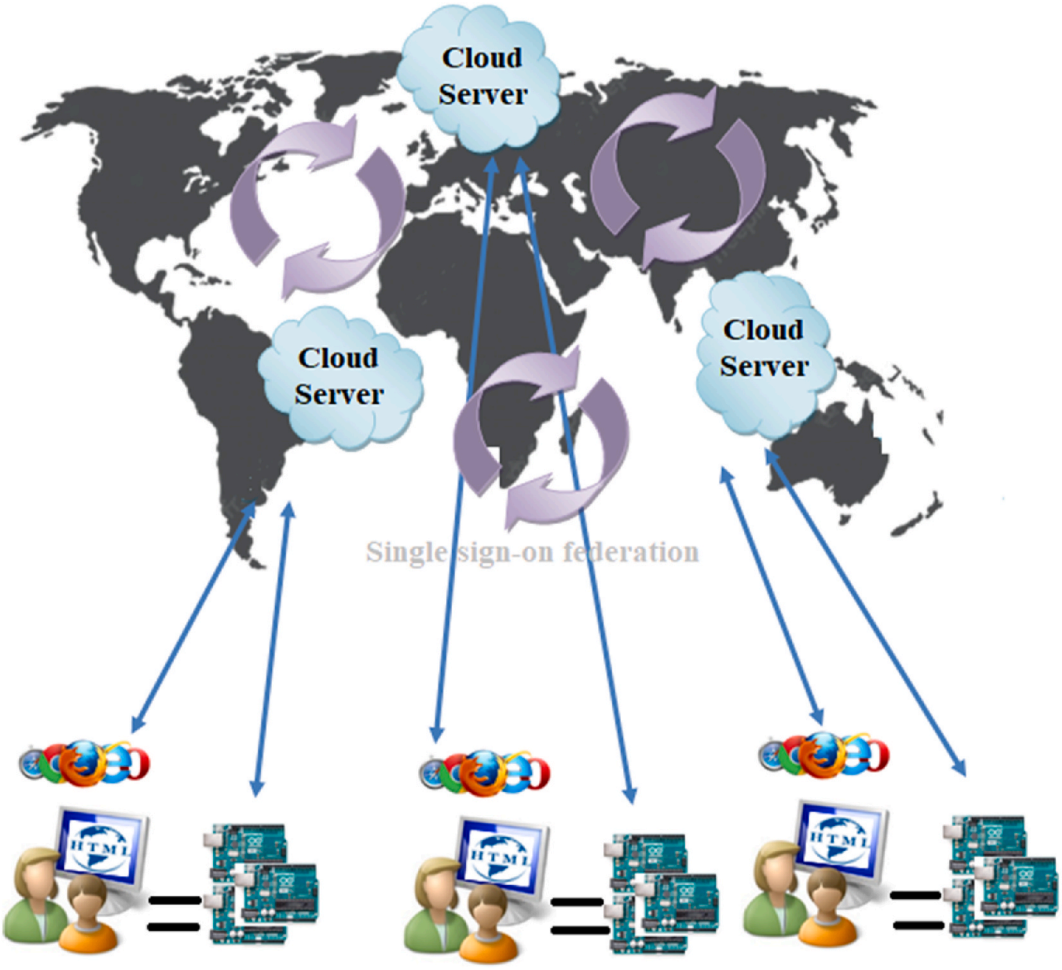

Fig. 2. A multi-cloud architecture.

4.1. IoT cloud-based architecture

On the IoT platform, a variety of technologies were active.These technologies could move from statelessness to statelessness restricted to unrestricted status, and have real-time systems that are difficult to have non-binding real-time systems.The physical IoT option was chosen up to virtual parts that could create and consume services on different internet domains.As a result, there will be billions of related things, making it difficult to sustain the IoT industry and requiring new methods for the safety and innovation of IoT elements.In our future world, all living things and non-living items would be part of the revolutionary IoT.Each element will have a location, an address, and an explanation available online.A consumer computer, for instance, would be aware of itself. The consumption system was aware of the composition, identity, and operation of physical counterparties, and can communicate with them and make independent decisions.IoT now embraces “anything, anyone, any service” in addition to technology “everywhere, anyway, anytime".With the emergence of IoT products and solutions across the globe, the current Internet is going through a fundamental transition.

IPV6 techniques were increasingly used to connect the current generation of machines and smart objects created in the domain of wireless sensor networks.The world as we know it is about to be transformed following the integration of IoT technologies with the Internet.Take into account the world’s abundance of IoT-based products that easily communicate with one another on Ipv6 platforms.This is followed by the security of the objects and the security of the data sent.The Internet, as we know it now, has developed a single method for protecting data and information and resisting hostile attacks.The Internet should be the world in which they made predictions, combined with integrated intelligent systems with limited resources.Therefore, we must follow the security guidelines that would form the basis for connections between IoT products.Security, privacy, stability, and authentication services form the foundation for all security-related communications.The network should also be protected from unauthorized access or other threats.The information stored in the sensor network was crucial.The sensor a node was required to physically protect and the information it was supposed to store needs to be encrypted.We have conceptualized IoT security as a multi-tier architecture where data could be protected at multiple layers.For further security control, the levels could be adjustable to the software option.

A new transverse layer frame that ensures efficient use of the customizable interface translation table with improved safety features has been described in Fig. 3. The aforementioned stack would interface with typical TCP/IP blocks.We would be able to reduce the necessary security bytes using IATT and security functionality, freeing up more bandwidth for actual applications to interact.We use a simple domotics technology as an example to describe our design.We could be considering home automation, in which case we would like to remotely control every device in a house. We would be able to control our wireless appliances and turn them on and off at the slightest degree of uncertainty or alarm.Thus, our proposed single transverse layer design could accomplish the ideal situation of home automation.In general, the IoT perspective argues that it cannot come from a single plan.We would develop IoT designs and security perspectives through many minor initiatives and specifications. Using internet services to the Internet of Things applications and the transition from IPv4 to IPv6. The IoT system has many benefits which should be explored. It would provide common platforms for the streamlined creation of cross-platform gadgets & enable a consistent structure of system implementation with gateways and Internet servers. The IoT is a sophisticated mix of homogeneous and heterogeneous technologies on several cross-layer interfaces, supplemented by a variety of third-party apps. Due to the lack of resources, it is crucial to study security methods and solutions and establish them as industry standards within the IoT space.

4.2. Security concern architecture

The layers of the stack that are used for end-to-end connectivity could be multiple strategies.We have covered some common security protocols for the different levels of the IoT stack.The connection layer requires recognition of the component implicated in the communication.There are no restrictions as to the number of terminals or hops that may be used in the interaction. A key was established before a conversation even begins. This secrecy would be used to secure each communication occurring in the communication process.The entire level of security has been compromised if this feature is compromised.The per-hop safety setup could identify unauthorized changes in each of the corresponding hops. 6LoWPAN connections, and transit security products, should guarantee data integrity. The purpose of the safety of the connecting layer is to ensure interaction between two nearby nodes.One of the adaptable choices could be utilized with a variety of procedures at levels above the link layers.

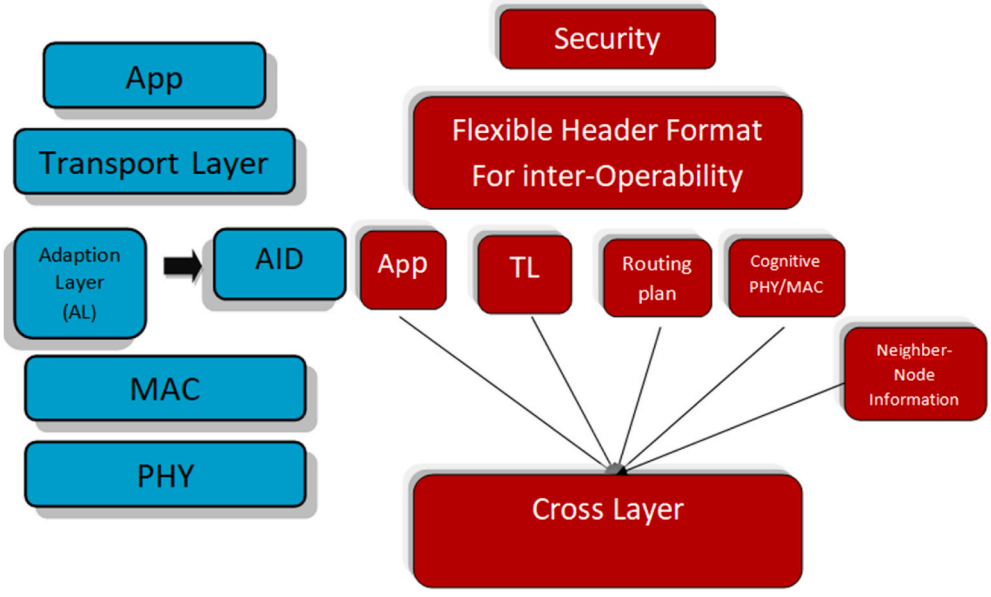

Fig. 3. Safety transverse structure.

A verification, validity, replay protection, & confidentiality as mentioned above, this scheme provides end-to-end protection.The IPsec method could be used for a variety of network-level transmission layer protocols, including TCP, UDP, HTTP, and CoAP.IPSec was a good option for a security solution, but it is generally inadequate when it comes to web protocols in terms of robustness.The most widely used methods for this were Secure Sockets Layer and Transport Layer Security.Only stream-oriented TCP can be used with the TLS protocol, which may not be the best choice for wireless connectivity.Only a stream-oriented TCP, which should be the ideal communication protocol for embedded smart objects, can be used.Another technique which would be a TLS for UDP adaptation was referred to as datagram TLS.The DTLS guarantees the full security of many programs.With the help of cookies in the field of the Internet interface, DTLS also offers defense against provider denial attacks.

With the aforementioned security measures in place, Internet attacks might still undermine the security of the channel.Many intrusion detection systems are capable of detecting malevolent activity and impostors in a system.To prevent undesirable network access, firewalls were required.There are billions of connected gadgets in the world of IoT, and they might contemplate being a piece of the simulated big bang universe.The 6LoWPAN IoT systems are prone to numerous attacks from the web and connection.The wireless domain of the Internet of Things, which has resource constraints, has successfully hacked the traditional Internet.We would need separate IDS to provide greater protection for IoT-enabled devices.

It should be correct to conclude that by integrating different telecommunications and information security technologies, systems and communications have been protected.The next issue should be to safeguard any information that IoT devices may contain.Data storage on an IoT device can contain sensitive or confidential information that must be protected.The Internet of Things was composed of tiny, clumps of goods. It should be difficult to manually secure or use trusted platform components on any of these billions of devices.

4.3. Registration strategies of IoT devices join the cloud

The IoT device can utilize one of two separate recording techniques, for example, the enhanced Arduino Yun with security features.

- Case A, with no supervision: automated MAC address and obH certification;
- Case B, end-user MAC address, and obH web registration were monitored.

In all situations, the end user should enable the WPS button on his wireless PA to allow the IoT device to preserve the WiFi network connection.This means that after performing the verification described in Section 4, the IoT device could connect to the Internet.In scenario B, an orange LED flashes on the IoT device circuit, and after incomplete identification, it shows a fixed orange LED.When the end-user establishes a link between the IoT device card and their web profile, full certification is achieved.To register the card, the customer uses a web page, by entering the MAC address which would be printed on the operator's box outside.By using the WPS button on his wireless AP, the end user should allow the IoT device to keep the WiFi network connection in both situations.Accordingly, the IoT device can connect to the network and perform the check. In Example B, the IoT device board blinks on an orange LED and, after partial registration, displays a fixed orange LED. The end user connects the IoT device card to their web profile to supplement the application.The user selects a web page to enroll the board of directors, using the MAC address specifically as it appears on the product provided box outside.

5. Conclusions

A completely new approach to AITT, they have developed a secure cross-layer framework for the IoT.Future efforts should include the practical development of a home automation system.A network of heterogeneous and homogeneous devices constitutes the IoT.As far as IoT applications are concerned, security and confidentiality are the main concerns.These issues continue to present significant challenges, and the analysis of infrastructure and security features was examined.A key element of the multi-level architecture and safety challenges was addressed.The system could be modified by the concept of our work in the defense sector.Applications and system changes may be performed using adaptive identifiers to their security requirements.An attempt was made to provide a high-level overview of the safety of IoT-enabled products.

CRediT authorship contribution statement

G Soniya Priyatharsini: Writing – original draft, Validation. **A. Jyothi Babu:** Supervision, Writing – review & editing, Reviewing and Editing. **M. Gnana kiran:** Conceptualization. **SathishKumar P.J:** Data curation. **Nelson Kennedy Babu C:** Conceptualization. **Aleem Ali:** Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] A.I. Abdi, F.E. Eassa, K. Jambi, K. Almarhabi, M. Khemakhem, A. Basuhail, M. Yamin, Hierarchical blockchain-based multi-chaincode access control for securing IoT systems, Electronics 11 (5) (2022) 711.
[2] I. Singh, S.W. Lee, Self-adaptive and secure mechanism for IoT based multimedia services: a survey, Multimed. Tool. Appl. (2021) 1–36.
[3] T. Ragunthar, P. Ashok, N. Gopinath, M. Subashini, A strong reinforcement parallel implementation of k-means algorithm using message passing interface, Mater. Today Proc. 46 (2021) 3799–3802, https://doi.org/10.1016/j.matpr.2021.02.032.
[4] Q. Zhou, M. Xiao, L. Lu, J. Zeng, W. He, C. Li, Y. Shi, A data-secured intelligent IoT system for agricultural environment monitoring, Wireless Commun. Mobile Comput. 2022 (4518599) (2022), 2022.
[5] A.K. Gupta, C. Chakraborty, B. Gupta, Secure transmission of EEG data using watermarking algorithm for the detection of epileptical seizures, Trait. Du. Signal 38 (2) (2021) 473–479.
[6] H.B. Mahajan, A.S. Rashid, A.A. Junnarkar, N. Uke, S.D. Deshpande, P.R. Futane, B. Alhayani, Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems, Appl. Nanosci. (2022) 1–14.
[7] Saravanan Nallusamy, Subramani Appavupillai, Sivakumar Ponnusamy, Mobile agents based reliable and energy efficient routing protocol for MANET, Power 3 (2016) 12.
[8] V.K.S. Maddala, K. Jayarajan, M. Braveen, R. Walia, P. Krishna, S. Ponnusamy, K. Kaliyaperumal, Multisensor data and cross-validation technique for merging temporal images for the agricultural performance monitoring system, J. Food Qual. 2022 (9575423) (2022), 2022.
[9] S. Sharma, Securing IoT communications using blockchain technology, in: Blockchain Security in Cloud Computing, Springer, Cham, 2022, pp. 145–166.
[10] K.C. Albeshri Suresh, K. Sivaraman, Improvising the performance of wireless sensor networks by quality aware stream control transmission protocol, Int. J. Appl. Eng. Res. 9 (22) (2014) 5928–5936.
[11] T.P. Latchoumi, L. Parthiban, Quasi oppositional dragonfly algorithm for load balancing in cloud computing environment, Wireless Pers. Commun. 122 (3) (2022) 2639.
[12] T Thulasimani, D. Sundaranarayana, B Kannadasan, Ponnusamy Sivakumar, K. Pavithra, R. Salin, Analysis of vacancies on passenger bus in the context of IoT Transport Sector with Efficient Management Technologies, Journal of Optoelectronics 41 (3) (2022). https://gdzjg.org/index.php/JOL/article/view/92.
[13] S. Mayoof, H. Alaswad, S. Aljeshi, A. Tarafa, W. Elmedany, A hybrid circuits-cloud: development of a low-cost secure cloud-based collaborative platform for A/D circuits in virtual hardware E-lab, Ain Shams Eng. J. 12 (2) (2021) 1197–1209.

[14] G.N.R. Devi, S. Ponnusamy, J. Pandit, B. Buvaneswari, Development of medicinal industries in building A replica to the damaged human tissue for artificial organs with the application of micro-and nano technology (mnt), J. Optoelectron. - Laser 41 (3) (2022) 79–83.
[15] S.K. Chandrasekaran, P. Savarimuthu, P. Andi Elumalai, K. Ayyaswamy, Primary path reservation using enhanced slot assignment in tdma for session admission, Scientific World Journalthis link is disabled 2015 (2015), 405974.
[16] N.R. Kumar, M. Arun, Deep learning model to improve security in IOT systems, in: 2022 International Conference *on Smart Technologies And Systems For Next Generation Computing (ICSTSN)*, IEEE, 2022, March, pp. 1–5.
[17] S. Subashka Ramesh, D. Venkataraja, R. Nikhil Bharadwaj, M.V. Santhosh Kumar, S. Santhosh, E-voting based on block chain technology, Int. J. Eng. Adv. Technol. 8 (5) (2019) 107–109.
[18] K. Sridharan, P. Sivakumar, A systematic review on techniques of feature selection and classification for text mining, Int. J. Bus. Inf. Syst. 28 (4) (2018) 504–518.
[19] M. Monica, P. Sivakumar, S.J. Isac, K. Ranjitha, PMSG based WECS: control techniques, MPPT methods and control strategies for standalone battery integrated system, 1, in: AIP Conference Proceedings, vol. 2405AIP Publishing LLC, 2022, April, 040013.
[20] B. Karnan, A. Kuppusamy, Graph theory and matrix approach for machinability enhancement of cryogenic treated cobalt bonded tungsten carbide inserts, Journal homepage 39 (4) (2021) 1372–1382. *http://iieta.org/journals/ijht*.
[21] M.S. Minu, R. Aroul Canessane, S.S. Subashka Ramesh, Optimal squeeze net with deep neural network-based arial image classification model in unmanned aerial vehicles, Trait. Du. Signal 39 (1) (2022) 275–281.
[22] S.S. Subashka Ramesh, N. Hassan, A. Khandelwal, R. Kaustoob, S. Gupta, Analytics and machine learning approaches to generate insights for different sports, Int. J. Recent Technol. Eng. 7 (6) (2019) 1612–1617.
[23] D.K. Sharma, K.K. Bhardwaj, S. Banyal, R. Gupta, N. Gupta, L. Nkenyereye, An opportunistic approach for cloud service-based IoT routing framework administering data, transaction, and identity security, IEEE Internet Things J. 9 (4) (2021) 2505–2512.
[24] H. Song, C.E. Montenegro-Marin, Secure prediction and assessment of sports injuries using deep learning based convolutional neural network, J. Ambient Intell. Hum. Comput. 12 (3) (2021) 3399–3410.