STM JOURNALS

Journal of
VLSI Design Tools & Technology

https://journals.stmjournals.com/jovdtt

ISSN: 2249-474X (Online)
ISSN: 2321-6492 (Print)
Volume 15, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoVDTT

Review JoVDTT

Robust Access Control Mechanisms Using VHDL Programming for IoT Security

Jadhav Vaibhavi Kishor[1,*], Kazi Kutubuddin Sayyad Liyakat[2]

Abstract

The Internet of Things (IoT) devices are increasingly becoming targets for criminal actors. A compromised device can result in data breaches, denial-of-service attacks, and even physical damage. While software-based security solutions are important, they are susceptible to attacks and often impose significant overhead, negatively impacting both performance and battery life. A viable alternative is provided by hardware-based security, which takes advantage of the inherent security benefits that are associated with dedicated hardware implementations. It is possible to greatly reduce the number of vulnerabilities that can be exploited through software by integrating security capabilities directly into the hardware. Virtual Hardware Description Language (VHDL) is a powerful language that enables designers to develop individualized hardware implementations that are tailored to specific security requirements. The growth of IoT devices necessitates the implementation of stringent security measures to protect sensitive data and prevent unauthorized access. This study investigates whether it is possible to use VHDL to construct hardware-based access control methods in IoT systems, as well as whether this approach is effective. A unique architecture for a VHDL-based access control module that is both flexible and resource-efficient is proposed by us. We demonstrate that this architecture has the capability to implement fine-grained access control regulations with low performance overhead. When compared to traditional software-based solutions, the results of the simulation demonstrate a considerable reduction in vulnerability to common software threats. Additionally, we conduct an analysis of the proposed VHDL implementation's space and power consumption, highlighting the fact that it is suitable for IoT contexts that are limited in terms of resources. A strong argument is presented in this work to support the incorporation of hardware-based access control as an essential layer of defense in the process of protecting the IoT landscape.

Keywords: Internet of Things, security, VHDL, VHDL programming, robust access control

***Author for Correspondence**
Jadhav Vaibhavi Kishor
E-mail: vaibhavij309@gmail.com

[1]Student, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology (BMIT), Solapur, Maharashtra, India
[2]Professor and Head, Department of Electronics and Telecommunication Engineering, Brahmdevdada Mane Institute of Technology (BMIT), Solapur, Maharashtra, India

Received Date: May 13, 2025
Accepted Date: May 14, 2025
Published Date: August 21, 2025

Citation: Jadhav Vaibhavi Kishor, Kazi Kutubuddin Sayyad Liyakat. Robust Access Control Mechanisms Using VHDL Programming for IoT Security. Journal of VLSI Design Tools & Technology. 2025; 15(2): 6–19p.

INTRODUCTION

The landscape of the Internet of Things (IoT) is rapidly developing, connecting an increasing number of devices and producing enormous amounts of data. Nevertheless, this interconnection also creates substantial problems for system security. The practice of restricting access to resources based on the identification of the user and authorization is known as access control, and it is an essential component of IoT security. Although software-based access control techniques are quite widespread, hardware-based solutions, particularly those that are implemented using VHDL (VHSIC Hardware Description Language (VHDL)), provide a layer of protection that is both robust and resistant to tampering [1–10].

According to numerous studies [11–21], this study investigates the use of VHDL programming to build and implement access control mechanisms specifically designed to meet the restrictions and security requirements of IoT devices. Despite its adaptability, software-based access control is vulnerable to a wide range of attacks, including malware, code injection, and privilege escalation. These vulnerabilities can be more severe in IoT devices with limited resources. Hardware-based access control offers several significant advantages.

- *Resistance to tampering:* When access control logic is implemented directly within the hardware, it is substantially more difficult to compromise than when software is used.
- *Enhanced security:* Hardware-level security offers an additional layer of protection, prohibiting unauthorized access even if the software layer is breached.
- *Deterministic performance:* Hardware-based solutions provide a performance that is both predictable and consistent, which is essential for applications that operate in real-time IoT environments.
- *Decreased software overhead:* The software burden on IoT devices decreases when access control operations are offloaded to hardware. This frees up resources that may be used for other essential functions.

For modelling and imitating digital logic circuits, a strong hardware description language known as VHDL is used. The ability to specify the behavior and organization of hardware components is provided to inventors, which enables the development of individualized access control methods that are customized to the requirements of certain IoT devices [22–32].

The creation of a dedicated hardware module that enforces access rules based on attributes such as the following is required to implement access control in VHDL. User Authentication refers to the process of verifying the identification of an entity requesting access. Comparing a digital signature or password that has been stored is one way to accomplish this.

The process of assigning employers to roles that have specified permissions is referred to as role-based access control (RBAC). After determining the role of the user requesting access, the VHDL module allows access in accordance with this role.

The process of defining access rules based on multiple properties of the user, the resource being accessed, and the environment is referred to as attribute-based access control (ABAC). As a result, a more granular and adaptable access control mechanism is brought about. The practice of restricting access to properties depending on the time of day or the day of the week is referred to as time-based access control.

A VHDL module for a fundamental RBAC system is demonstrated in the following simplified example:

```
library Institute of Electrical and Electronics Engineers (IEEE);
use ieee.std_logic_1164.all;

entity AccessControl is
  Port (
    user_role: in std_logic_vector(1 to 0);  -- User's role (e.g., 00=Guest, 01=User, 10=Admin).
    resource_id : in  std_logic_vector(1 downto 0);  -- Resource being accessed
    access_granted: out std_logic
  );
end AccessControl;

architecture Behavioral of AccessControl is
```

ISSN: 2249-474X (Online), ISSN: 2321-6492 (Print)

```
begin
   process (user_role, resource_id)
   begin
      case resource_id is
         when "00" =>  -- Resource 1 requires Admin access
            if user_role = "10" then
               access_granted <= '1';
            else
               access_granted <= '0';
            end if;
         when "01" =>  -- Resource 2 requires User or Admin access
            if user_role = "01" or user_role = "10" then
               access_granted <= '1';
            else
               access_granted <= '0';
            end if;
         when others => -- All other resources require Guest access
            if user_role = "00" or user_role = "01" or user_role = "10" then
               access_granted <= '1';
            else
               access_granted <= '0';
            end if;
      end case;
   end process;
end Behavioral;
```

An example of a basic access control module written in VHDL is shown in the following code snippet. The entity is named AccessControl in the file. It has input ports for user_role and resource_id and an output port named access_granted. Whether access should be given is determined by the module, based on the user's role and the resource being accessed [33–43].

Within an IoT device, the VHDL code that represents the access control module is often synthesized and implemented on a Field-Programmable Gate Array (FPGA) or an Application-Specific Integrated Circuit (ASIC). This makes it possible to accomplish tight integration with the hardware architecture of the device and guarantees that the logic for access control is carried out effectively.

Although access control based on VHDL presents several compelling advantages, a number of issues must be addressed:

- *Complexity:* The design of complex access control methods in VHDL can be difficult and require specialized knowledge and experience.
- Because IoT devices frequently have limited resources, the VHDL-based access control module needs to be developed in such a way that it is both efficient and consumes the least number of resources.
- *Flexibility:* Although hardware-based access control provides a higher level of protection, it may be less versatile than software-based methods. A thorough consideration should be given to the possibility that there is a need for future upgrades and alterations.
- *Formal Verification:* It is essential to perform exhaustive testing and formal verification to guarantee the correctness and safety of the VHDL code, thereby reducing the likelihood of any potential vulnerabilities.

Regarding IoT security, VHDL programming offers a powerful tool that can be used to design access control mechanisms that are temperature resistance and robust. IoT devices can achieve a higher level of security, protect sensitive data, and alleviate concerns associated with unauthorized access when they use hardware solutions. The VHDL-based access control strategy is a beneficial method for safeguarding the ever-expanding IoT, even though there are hurdles to be faced. The benefits of better security and deterministic performance render this approach useful. VHDL and other hardware description languages will play an increasingly important role in the construction of a safer and more trustworthy connected world [44–54]. This is because the demand for secure IoT devices is expected to continue growing.

THE ROLE OF VHDL PROGRAMMING IN SECURING IoT WITH ACCESS CONTROL MECHANISMS

The IoT has revolutionized many different industries, ranging from residential automation to small-scale industrial automation. However, there are substantial security challenges associated with this interconnection. One of the most important aspects of IoT security is the implementation of robust access control mechanisms, and very-high-speed integrated circuit Hardware Description Language (VHDL) programming is playing an increasingly important role in accomplishing this goal [55–65].

IoT techniques are typically employed in contexts with inadequate physical security and are frequently constrained by resource constraints. The combination of these qualities, along with the possibility of large-scale deployments, makes them appealing targets for cyberattacks. In the absence of adequate access control, malevolent actors have the following abilities.

- Compromise the operation of devices by controlling them to interrupt services, alter data, or even physically damage equipment.
- Accessing personal information, financial data, or intellectual business secrets that are transferred or stored by IoT devices provides an opportunity to steal sensitive data.
- Using susceptible devices as part of a botnet, launch distributed denial-of-service attacks (DDoS) to overwhelm the target servers.
- Acquire unauthorized access to networks by employing hacked devices as gateways to penetrate more protected internal networks.

Consequently, the implementation of efficient access control is of the utmost importance to mitigate these dangers. Within an IoT ecosystem, access control systems are responsible for determining who is permitted to access resources. These mechanisms range from straightforward password authentication to more complex mechanisms such as RBAC and ABAC.

Hardware-based implementations utilizing VHDL offer various advantages, particularly in resource-constrained and security-critical IoT scenarios. Software-based solutions for access control are ubiquitous, whereas hardware-based implementation offers several advantages.

Hardware implementations are more resistant to software-based assaults, such as buffer overflows and code injections, which can circumvent software-based security methods. This is one of the reasons why hardware implementations offer enhanced security. VHDL provides developers with the ability to rigorously control the behavior of hardware, thereby reducing the number of vulnerabilities.

- *Enhancement of performance:* When compared to software, the execution of access control logic in hardware results in much quicker processing speeds. Real-time IoT applications, in which latency is of the utmost importance, require this.
- *Resource efficiency:* VHDL makes it possible to create highly optimized circuits that use less power and memory. This is a critical feature of IoT devices that are powered by batteries or have limited resources.
- *Tamper resistance:* Hardware implementations can be made more tamper-resistant by physically safeguarding the integrated circuit (IC) on which the VHDL code is implemented. This is one way to achieve this goal. Because of this, unauthorized access and alteration are prevented.

ISSN: 2249-474X (Online), ISSN: 2321-6492 (Print)

- *Adaptability:* VHDL offers the freedom to develop individualized access control methods customized to the specific requirements and limitations of IoT applications.

Within IoT devices and gateways, VHDL can be utilized to construct a variety of access control techniques, including the following.

- *Hardware security modules (HSMs):* VHDL programs can define the functioning of cryptographic processors that are contained within HSMs. These HSMs are used for encryption, authentication, and secure key storage. Consequently, this safeguards sensitive data and guarantees that only authorized devices can access it.
- The implementation of secure boot processes in VHDL ensures that only authorized and authenticated firmware can be loaded onto the device. This is referred to as "secure boot implementation." By doing so, malicious firmware can be prevented from being installed, which would otherwise compromise the system.
- *Hardware-based authentication:* VHDL can be utilized to develop hardware-based authentication methods such as physical unclonable functions (PUFs) or other methods that generate one-of-a-kind fingerprints for secure identification.
- *Access control lists (ACLs):* VHDL implementations can control access to hardware peripherals or memory areas based on specified access control lists. This prevents unauthorized modifications or access to hardware.
- *Role-based access control:* The VHDL code can enforce RBAC policies by defining roles and privileges and restricting access to resources based on the role assigned to a user or device.

When it comes to implementing access control in the IoT, VHDL presents a number of major advantages; nevertheless, there are also problems to consider:

- *Complexity:* Programming in VHDL can be difficult and often requires specialized knowledge and skills.
- In terms of development time, the hardware development process can be more time-consuming than the software development process.
- *Cost:* The development of hardware and prototyping of hardware can be more expensive than the development of software.

The development of VHDL tools and approaches that are more user-friendly is driven by the growing demand for secure and dependable IoT devices, despite the challenges presented. Among the upcoming trends are the following.

- *High-level synthesis (HLS):* HLS tools facilitate hardware development by automatically translating high-level programming languages such as C++ into VHDL code.
- *Security-aware design automation:* Tools that enable automatic identification and mitigation of security vulnerabilities in VHDL code are becoming an increasingly significant component of the design process.
- *Integration with software-defined networking (SDN):* When VHDL-based access control is combined with SDN, it is possible to implement dynamic and adaptable security rules for large-scale IoT installations.

Programming in VHDL is an essential component in the protection of IoT devices and systems, because it enables the construction of access control methods that are both reliable and effective. Even though there are still obstacles to overcome, the advantages of hardware-based security, performance, and resource efficiency make VHDL an indispensable instrument for safeguarding the expanding IoT environment. The significance of VHDL in the construction of trustworthy and secure IoT solutions will only continue to increase as the number of cyberattacks targeting IoT devices continues to increase in both number and sophistication.

SECURING IoT LEVERAGING VHDL FOR ROBUST ACCESS CONTROL

IoT is rapidly revolutionizing our environment by linking a large number of devices and making it possible to use a wide variety of resources. This interconnection results in serious security risks. To prevent unauthorized access, manipulation, and data breaches, access control, which is a fundamental security function, becomes even more important in the context of the IoT ecosystem. This section investigates the design and implementation of access control mechanisms utilizing VHDL, which is a hardware description language. This language provides a method that is both reliable and secure for protecting IoT devices and networks [66–70].

IoT devices collect sensitive data and control vital infrastructure on a regular basis. In the absence of adequate access control, malevolent actors have the following abilities.

- *Compromise Device Functionality:* This involves gaining control of devices and manipulating their function, which may result in system failures or even physical harm.
- *Steal Sensitive Data:* Gain access to and steal confidential company information, financial data, or personal information while stealing sensitive data.

To launch DDoS attacks, compromised devices can be used as bots in DDoS attacks, which overload network resources and interrupt services. Impersonating authorized users allows them to gain access to systems and data. This is accomplished by impersonating authorized users.

Traditional access control systems based on software can be susceptible to software exploits and malicious software. Hardware-based solutions provide an alternative that is more secure because they embed access control logic directly into the hardware of the device. This makes it more difficult to manipulate hardware.

Designing access control methods in hardware can be accomplished with the help of VHDL, which is the VHSIC Hardware Description Language. This language is powerful and versatile. Therefore, this is an attractive option for IoT security.

- *Security at the hardware-level:* VHDL enables the design of bespoke hardware logic, which guarantees that access control rules are directly applied to the silicon of the device. This provides a better level of security compared to software solutions.
- *Performance and Efficiency:* VHDL designs can be optimized for performance, which enables speedy access control choices without introducing considerable potential (also known as "performance optimization"). IoT applications that operate in real time require this technology.
- *The ability to be customized:* VHDL makes it possible to fabricate access control mechanisms that are highly customized and personalized to meet the specific requirements of IoT devices or applications. Within this context, definitions of roles, permissions, and authentication mechanisms are included.
- *Implementation flexibility:* VHDL designs can be implemented on multiple hardware platforms, including FPGAs and ASICs, offering flexibility in terms of cost, performance, and power consumption.
- *Formal verification:* VHDL designs can be formally verified to ensure that they do not include any vulnerabilities and that they meet established security requirements.

The following procedures are commonly involved in the construction of a VHDL-based access control mechanism, comparable to those depicted in Figure 1.

1. *Defining security requirements:* Determine the precise security requirements of IoT devices and applications. These requirements include the types of resources that need to be safeguarded, the roles and permissions of various users or devices, and authentication techniques that will be utilized.

Journal of VLSI Design Tools & Technology
Volume 15, Issue 2
ISSN: 2249-474X (Online), ISSN: 2321-6492 (Print)

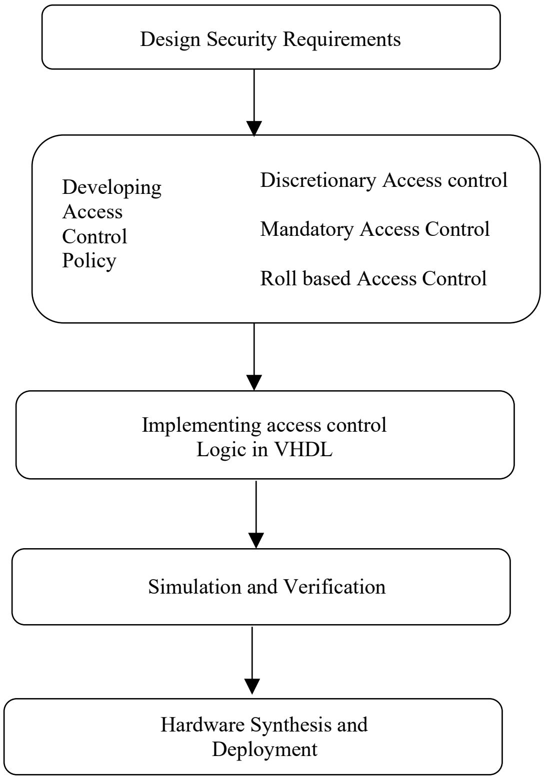

Figure 1. Designing steps.

2. Developing an access control policy defines a formal access control policy that outlines the rules for granting or denying access to resources based on the identification of the person making the request and the operation being requested. Common simulations of access control include the following.
   - *Discretionary access control (DAC)* is a system in which owners of resources have the authority to decide whether additional users should be granted access.
   - *Mandatory access control (MAC):* The results of access control are based on security measures that are applied to both the themes (employers or procedures) and the objects (resources).
   - Employers are allocated roles, and roles are provided with permission to access resources. This type of access control is referred to as RBAC.
3. *Putting access control logic into action in a VHDL framework:* The access control policy should be translated into VHDL code instead. To accomplish this, logic circuits capable of performing authentication, authorization, and audit logging must be designed.
4. *Simulation and verification:* To guarantee that the VHDL design satisfies the security criteria and does not present any flaws or vulnerabilities, it is necessary to perform a comprehensive simulation and verification of the design. It is possible to obtain a high level of confidence using formal verification techniques.
5. *Synthesis and deployment of hardware:* This step involves converting the VHDL code into a hardware implementation, which can be performed on either an FPGA or ASIC. After the hardware has been deployed to the IoT device, it should be configured to enforce an access control policy.

To illustrate the fundamental ideas behind the implementation of an RBAC system in VHDL using the following simple example:

```
entity AccessControl is
    Port (
```



```
    UserID  : in  std_logic_vector(7 downto 0);  -- User Identifier
    ResourceID : in  std_logic_vector(7 downto 0);  -- Resource Identifier
    Operation: in  std_logic_vector(2 to 0);  operation (e.g., Read, Write, Execute)
    GrantAccess : out std_logic
  );
end AccessControl;

architecture Behavioral of AccessControl is

  type RolePermissionsArray is an array (0–255, 0–255, 0–7) of std_logic;
  signal RolePermissions : RolePermissionsArray;

  Initialize RolePermissions (Example: Role 1 can Read Resource 1)
  attribute INIT : string;
  attribute INIT of RolePermissions: signal is' "(others => (others => (others => '0'))), (1, 1, 0 => '1')"

begin

  process (UserID, ResourceID, Operation)
  begin
    if RolePermissions(conv_integer(UserID), conv_integer(ResourceID), conv_integer(Operation))
= '1' then
      GrantAccess <= '1';
    else
      GrantAccess <= '0';
    end if;
  end process;

end Behavioral;
```

The purpose of this example is to demonstrate a fundamental RBAC implementation in which RolePermissions stores the access rights for each role (UserID) on each resource for a variety of operations. The logic for role management, authentication, and policy updates in real-world systems is more complicated than that shown here, which is a significantly simplified form. To illustrate how VHDL can be utilized to create a fundamental RBAC system, the following is a simplified example:

```
entity rbac_controller is
 Port ( user_id : in std_logic_vector(7 downto 0);
       resource_id: in std_logic_vector(7 downto 0);
       access_type: in std_logic_vector(1 downto 0); -- e.g., read, write
       granted: out std_logic);
end rbac_controller;

architecture Behavioral of rbac_controller is
 type role_permissions is an array (0 to 255, 0 to 255) of std_logic_vector(1 to 0);
 Signal permissions: role_permissions: = (others = > (others => (others => "00")); -- default denial)

begin
 process(user_id, resource_id, access_type)
 begin
  In reality, this would likely involve database lookup.
  or more sophisticated access-control policies.

  Example: User with ID "10" has read access to resource "20."
```



```
    if user_id = "00001010" and resource_id = "00010100" and access_type = "01" then -- Read = "01"
      granted <= '1';
    else
      granted <= '0';
    end if;
  end process;
end Behavioral;
```

This streamlined illustration demonstrates how VHDL can be utilized to build access control rules that are based on the IDs of both users and resources. A more comprehensive implementation would require a more in-depth review of the policy, as well as the possibility of utilizing external data sources for information regarding users and roles.

Although VHDL provides a solid basis for secure control of IoT access, there are a few obstacles that need to be overcome.

- *Complexity:* Designing complex access control mechanisms in VHDL can be difficult and will take a significant amount of time.
- Integration is a process that requires careful planning and implementation to successfully integrate VHDL-based access control with other security components, such as encryption and intrusion detection systems.
- *Dynamic policy updates:* The process of implementing methods for dynamically changing access control policies in hardware can be difficult and involves careful consideration of the trade-offs between performance and security.
- *Consumption of power:* Hardware-based access control can consume a large amount of power, which is an issue for IoT devices that are powered by batteries.

Possible future paths for research include:

- The use of HLS tools to automatically produce VHDL code from higher-level descriptions of access control policies simplifies the design process. This is referred to as HLS.
- The development of more robust formal verification techniques to verify the correctness and security of VHDL-based access control mechanisms is the focus of formal methods development projects.
- Techniques for lowering the amount of power consumed by hardware-based access control are being investigated as part of an energy-efficient design project.
- *Hardware security modules:* Integrating VHDL-based access control with exclusively dedicated HSMs to provide a higher level of security.

VHDL offers a tool that is both resilient and versatile for building safe access control mechanisms for IoT devices and networks. VHDL provides a better level of security than software-based solutions because it can embed access control circuitry directly in hardware. Even though obstacles remain to be overcome, continuous research efforts are gradually improving the capabilities and applicability of VHDL in terms of protecting the ever-expanding world of IoT. The significance of secure access control, particularly through hardware-based solutions such as those created with VHDL, will become even more crucial as reliance on IoT continues to expand.

CONCLUSION

Through this investigation, it was demonstrated that the utilization of VHDL has a large potential for the implementation of access control mechanisms that are both reliable and effective within IoT devices that have limited resources. Compared to typical software-based techniques, the VHDL-based ACL module that has been suggested offers a proven improvement in security. It provides enhanced tamper resistance and reduces vulnerability to popular attack routes. According to the findings, solutions based on VHDL provide a realistic avenue for safeguarding IoT frontiers by incorporating security functionalities directly into the hardware fabric. To further streamline the development process and improve the scalability of these systems, future research should focus on investigating the possibility of integrating more complex cryptographic algorithms and developing automated tools for the generation and verification of VHDL-based access control modules. Additionally, it is necessary to conduct practical testing on real-world IoT platforms to validate these theoretical models and evaluate their performance under realistic operating settings. Finally, the adoption of hardware-centric security approaches powered by VHDL is necessary to construct an IoT environment that is trustworthy and safe.

REFERENCES

1. Jadhav M, Nerkar PM. FPGA-based finger vein recognition system for personal verification. Int J Eng Res Gen Sci. 2015;3:382–8.
2. Nerkar PM, Shinde SS, Liyakat KK, Desai S, Kazi SS. Monitoring fresh fruit and food using IoT and machine learning to improve food safety and quality. Tuijin Jishu J Propuls Technol. 2023;44:2927–31.
3. Khadake S, Kawade S, Moholkar S, Pawar M. A review of 6G technologies and its advantages over 5G technology. In: Pawar PM, Ronge BP, Gidde RR, Pawar MM, Misal ND, Budhewar AS, More VV, Reddy PV, editors. Techno-Societal 2022: Proceedings of the 4th International Conference on Advanced Technologies for Societal Applications – Volume 1. New York: Springer International Publishing; 2024. p. 1043–51. doi:10.1007/978-3-031-34644-6_107.
4. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, Sawant VA. Review of AI in power electronics and drive systems. 2024 3rd International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC), Mathura, India. 2024. p. 94–9. doi:10.1109/PARC59193.2024.10486488.
5. Dudgikar AB, Ingalgi AAA, Jamadar AG, Swami OR, Khadake SB, Moholkar SV. Intelligent battery swapping system for electric vehicles with charging stations locator on IoT and cloud platform. Int J Adv Res Sci Commun Technol. 2023;3:204–8. doi:10.48175/IJARSCT7867.
6. Khadake SB, Patil VJ. Prototype design & development of solar based electric vehicle. 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India. 2023. p. 1–7. doi:10.1109/SMARTGENCON60755.2023.10442455.
7. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, Sawant VA. A comprehensive analysis of artificial intelligence integration in electrical engineering. 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Lalitpur, Nepal. 2024. p. 484–91. doi:10.1109/ICMCSI61536.2024.00076.
8. Khadake SB, Dolli SP, Rathod KS, Waghmare OP, Deshpande AV. An overview of intelligent traffic control system using PLC and use of current data of vehicle travels. JournalNX. 2021 Jan 31;:1-4. Available from: https://repo.journalnx.com/index.php/nx/article/view/739.
9. Magar SS, Sugandhi AS, Pawar SH, Khadake SB, Mallad HM. Harnessing wind vibration, a novel approach towards electric energy generation – Review. Int J Adv Res Sci Commun Technol. 2024;4:73–82. doi:10.48175/IJARSCT-19811.
10. Khadake SB, Padavale PV, Dhere PM, Lingade BM. Automatic hand dispenser and temperature scanner for COVID-19 prevention. Int J Adv Res Sci Commun Technol. 2023;3:362–7. doi:10.48175/IJARSCT11364.
11. Landage SS, Chavan SR, Kokate PA, Lohar SP, Pawar MK, Khadake S. Solar outdoor air purifier with air quality monitoring system. In: Synergies of Innovation: Proceedings of NCSTEM 2023; 2023 September; Pandharpur, India. 2024. p. 260–266.
12. Khadake SB. Detecting salient objects of natural scene in a video's using spatio-temporal saliency & colour map. JournalNX. 2021;2:30–5. Available from: https://repo.journalnx.com/index.php/nx/article/view/1070.
13. Khadake SB. Detecting salient objects in a video's by using spatio-temporal saliency & colour map. Int J Innov Eng Res .Technol. 2021;3:1–9. Available from: https://repo.ijiert.org/index.php/ijiert/article/view/910

14. Sawant VA, Bhosale PS, Kokare PD, Potdar DS, Waghmode SD. DTMF based irrigation water pump control system. Int Educ Res J. 2024 May;10(5):108-9.
15. Korake P, Murade H, Doke R, Narale V, Khadake SB, Chavan AS. Automatic load sharing of distribution transformer using PLC. Synergies of Innovation. 2024;253–9. Available from: https://www.researchgate.net/publication/383628063
16. Khadake SB, Kashid PJ, Kawade AM, Khedekar SV, Mallad HM. Electric vehicle technology battery management - Review. Int J Adv Res Sci Commun Technol. 2023;3:319–25. doi:10.48175/IJARSCT-13048.
17. Khadake SB, Chounde A, Gopnarayan BB, Patil KB, Kamble SS. Human Health Care System: A New Approach towards Life. Grenze Int J Eng Technol. 2024 Jun 15;10(2):5487–94.
18. Khadake SB, Patil VJ, Mallad HM, Gopnarayan BB, Patil KB. Maximize farming productivity through Agriculture 4.0 based intelligence, with use of Agri Tech Sense advanced crop monitoring system. Grenze Int J Eng Technol. 2024;10(2):5127–34.
19. Khedekar SV, Kawade AM, Vyavahare SS, Kashid PJ, Chounde AB, Mallad HM. Solar based electric vehicle charging system - Review. Int J Adv Res Sci Commun Technol. 2024;4:42–57. doi:10.48175/IJARSCT-22705.
20. Randive AB, Gaikwad SK, Khadake SB, Mallad HM. Biodiesel: A renewable source of fuel. Int J Adv Res Sci Commun Technol. 2024;4:225–40. doi:10.48175/IJARSCT-22836.
21. Sayyad L, Kazi K, Khadake SB, Chounde AB, Suryagan AA, Mallad HM, Khadatare MR. AI-Driven-IoT (AIIoT) based decision making system for high-blood pressure patient healthcare monitoring. 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India. 2024. p. 96-102. doi:10.1109/ICSCNA63714.2024.10863954.
22. Mulani AO, Bang AV, Birajadar GB, Deshmukh AB, Jadhav HM. IoT-based air, water, and soil monitoring system for pomegranate farming. Ann Agri Bio Res. 2024;29:71–86.
23. Parihar B, Kiran A, Valaboju S, Rashid SZ, Liyakat KKS, DR ASL. Enhancing data security in distributed systems using homomorphic encryption and secure computation techniques. ITM Web Conf. 2025;76:02010. doi:10.1051/itmconf/20257602010.
24. Veena C, Sridevi M, Liyakat KKS, Saha B, Reddy SR, Shirisha N. HEECCNB: An efficient IoT-cloud architecture for secure patient data transmission and accurate disease prediction in healthcare systems. 2023 Seventh International Conference on Image Information Processing (ICIIP), Solan, India. 2023. p. 407–10. doi:10.1109/ICIIP61524.2023.10537627.
25. Tamboli DA, Sawant VA, MHM, Sathe S. AI-driven-IoT(AIIoT) based decision-making – KSK approach in drones for climate change study. 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India. 2024. p. 1735–44. doi:10.1109/ICUIS64676.2024.10866450.
26. Prasad KR, Karanam SR, Ganesh D, Liyakat KKS, Talasila V, Purushotham P. AI in public-private partnership for IT infrastructure development. J High Technol Manag Res. 2024;35:100496. doi:10.1016/j.hitech.2024.100496.
27. Liyakat KKS. Detecting malicious nodes in IoT networks using machine learning and artificial neural networks. 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India. 2023. p. 1–5. doi:10.1109/ESCI56872.2023.10099544.
28. Kasat K, Shaikh N, Rayabharapu VK, Nayak M, Sayyad Liyakat KK. Implementation and recognition of waste management system with mobility solution in smart cities using Internet of Things. 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India. 2023. p. 1661–5. doi:10.1109/ICAISS58487.2023.10250690.
29. Kazi K. AI-driven IoT (AIIoT) in healthcare monitoring. In: Nguyen TVT, Vo NTM, editors. Using Traditional Design Methods to Enhance AI-Driven Decision Making. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 77–101. doi:10.4018/979-8-3693-0639-0.ch003.
30. Kazi K. Modelling and simulation of electric vehicle for performance analysis: BEV and HEV electrical vehicle implementation using Simulink for e-mobility ecosystems. In: LD N, Nagpal N, Kassarwani N, Varthanan V, Siano P, editors. E-Mobility in Electrical Energy Systems for

Sustainability. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 295–320. doi:10.4018/979-8-3693-2611-4.ch014.
31. Kazi KSL. Machine learning-powered IoT (MLIoT) for retail apparel industry. In: Tarnanidis T, Papachristou E, Karypidis M, Manda VK, editors. Sustainable Practices in the Fashion and Retail Industry. Hershey (PA): IGI Global Scientific Publishing; 2025. p. 345–72. doi:10.4018/979-8-3693-9959-0.ch015.
32. Kazi KSL. Braille-Lippi numbers and characters detection and announcement system for blind children using KSK approach: AI-driven decision-making approach. In: Murugan T, K P, Abirami AM, editors. Driving Quality Education Through AI and Data Science. Hershey (PA): IGI Global Scientific Publishing; 2025. p. 531–56. doi:10.4018/979-8-3693-8292-9.ch023.
33. Kazi KSL. AI-driven IoT (AIIoT)-based decision-making system for high BP patient healthcare monitoring: KSK1 approach for BP patient healthcare monitoring. In: Mzili T, Arya AK, Pamucar D, Shaheen M, editors. Optimization, Machine Learning, and Fuzzy Logic: Theory, Algorithms, and Applications. Hershey (PA): IGI Global Scientific Publishing; 2025. p. 71–102. doi:10.4018/979-8-3693-7352-1.ch003.
34. Kazi KSL. Advancing towards sustainable energy with hydrogen solutions: Adaptation and challenges. In: Özsungur F, Semsari MC, Küçük Bayraktar H, editors. Geopolitical Landscapes of Renewable Energy and Urban Growth. Hershey (PA): IGI Global Scientific Publishing; 2025. p. 357–94. doi:10.4018/979-8-3693-8814-3.ch013.
35. Kazi KSL. AI-driven-IoT (AIIoT) decision-making system for hepatitis disease patient healthcare monitoring: KSK1 approach for hepatitis patient monitoring. In: Agarwal S, Lakshmi D, Singh L, editors. Navigating Innovations and Challenges in Travel Medicine and Digital Health. Hershey (PA): IGI Global Scientific Publishing; 2025. p. 433–52. doi:10.4018/979-8-3693-8774-0.ch022.
36. Kazi KSL. Machine learning-based pomegranate disease detection and treatment. In: Ul Haq MZ, Ali I, editors. Revolutionizing Pest Management for Sustainable Agriculture. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 469–98. doi:10.4018/979-8-3693-3061-6.ch019.
37. Kazi KS. Computer-aided diagnosis in ophthalmology: A technical review of deep learning applications. In: Garcia MB, de Almeida RPP, editors. Transformative Approaches to Patient Literacy and Healthcare Innovation. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 112–35. doi:10.4018/979-8-3693-3661-8.ch006.
38. Kazi KSL. IoT driven by machine learning (MLIoT) for the retail apparel sector. In: Tarnanidis TK, Papachristou E, Karypidis M, Ismyrlis V, editors. Driving Green Marketing in Fashion and Retail. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 63–81. doi:10.4018/979-8-3693-3049-4.ch004.
39. Kazi KSL. AI-driven-IoT (AIIoT)-based decision making in drones for climate change: KSK approach. In: Aouadni S, Aouadni I, editors. Recent Theories and Applications for Multi-criteria Decision-Making. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 311–40. doi:10.4018/979-8-3693-6502-1.ch011.
40. Kazi KSL. Artificial intelligence (AI)-driven IoT (AIIoT)-based agriculture automation. In: Satapathy S, Muduli K, editors. Advanced Computational Methods for Agri-Business Sustainability. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 72–94. doi:10.4018/979-8-3693-3583-3.ch005.
41. Kazi KSL. Machine learning-driven Internet of Medical Things (ML-IoMT)-based healthcare monitoring system. In: Souene BO, Chakraborty C, editors. Responsible AI for Digital Health and Medical Analytics. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 49–86. doi:10.4018/979-8-3693-6294-5.ch003.
42. Kazi KSL. Transformation of agriculture effectuated by artificial intelligence-driven Internet of Things (AIIoT). In: Garwi J, Dzingirai M, Masengu R, editors. Integrating Agriculture, Green Marketing Strategies, and Artificial Intelligence. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 449–84. doi:10.4018/979-8-3693-6468-0.ch015.
43. KSK. Vehicle Health Monitoring System (VHMS) by employing IoT and sensors. Grenze Int J Eng Technol. 2024;10:5367–74. Available from: https://thegrenze.com/index.php?display=page&view=journalabstract&absid=3371&id=8.

44. KSK. A novel approach on ML based palmistry. Grenze Int J Eng Technol. 2024;10:5186–93. Available from: https://thegrenze.com/index.php?display=page&view=journalabstract&absid=3344&id=8
45. KSK. IoT based boiler health monitoring for sugar industries. Grenze Int J Eng Technol. 2024;10:5178–85. Available from: https://thegrenze.com/index.php?display=page&view=journalabstract&absid=3343&id=8
46. Keerthana R, KMV, Bhagyalakshmi K, Papinaidu M, VV, Liyakat KKS. Machine learning based risk assessment for financial management in big data IoT credit. SSRN Electron J. 2025. doi:10.2139/ssrn.5086671.
47. Kamaraj AK, Acharjya DP, editors. Explainable Artificial Intelligence in Healthcare Systems. New Delhi: Nova Publishers Science Publishers; 2024. doi:10.52305/GOMR8163.
48. Kazi KSL. Machine learning (ML)-based braille Lippi characters and numbers detection and announcement system for blind children in learning. In: Sart G, editor. Social Reflections of Human–Computer Interaction in Education, Management, and Economics. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 16–39. doi:10.4018/979-8-3693-3033-3.ch002.
49. Liyakat KKS. Machine learning approach using artificial neural networks to detect malicious nodes in IoT networks. In: Shukla PK, Mittal H, Engelbrecht A, editors. Computer Vision and Robotics. CVR 2023. Algorithms for Intelligent Systems. Singapore: Springer; 2023. p. 27–38. doi:10.1007/978-981-99-4577-1_3.
50. Liyakat Kazi KS. ChatGPT: An automated teacher's guide to learning. In: Bansal R, Chakir A, Hafaz Ngah A, Rabby F, Jain A, editors. AI Algorithms and ChatGPT for Student Engagement in Online Learning. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 1–20. doi:10.4018/979-8-3693-4268-8.ch001.
51. Kazi KSL. IoT technologies for the intelligent dairy industry: A new challenge. In: Thandekkattu SG, Vajjhala NR, editors. Designing Sustainable Internet of Things Solutions for Smart Industries. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 321–50. doi:10.4018/979-8-3693-5498-8.ch012.
52. Liyakat KKS. Heart health monitoring using IoT and machine learning methods. In: Shaik A, editor. AI-Powered Advances in Pharmacology. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 257–82. doi:10.4018/979-8-3693-3212-2.ch010.
53. Kazi KSL. AI-driven-IoT (AIIoT)-based decision making in kidney diseases patient healthcare monitoring: KSK approach for kidney monitoring. In: Polat LÖ, Polat O, editors. AI-Driven Innovation in Healthcare Data Analytics. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 277–306. doi:10.4018/979-8-3693-7277-7.ch009.
54. Liyakat KKS. Machine learning approach using artificial neural networks to detect malicious nodes in IoT networks. In: Udgata SK, Sethi S, Gao XZ, editors. Intelligent Systems. ICMIB 2023. Lecture Notes in Networks and Systems. Vol 728. Singapore: Springer; 2024. p. 137-48. doi: 10.1007/978-981-99-3932-9_12.
55. Pradeepa M, Jamberi K, Sajith S, Bai MR, Prakash A, Kazi KSL. Student health detection using a machine learning approach and IoT. 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India. 2022. doi:10.1109/MysuruCon55714.2022.9972445.
56. Kazi KSL, Mahant MA. Machine learning-driven Internet of Things (MLIoT)-based healthcare monitoring system. In: Wickramasinghe N, editor. Digitalization and the Transformation of the Healthcare Sector. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 205–36. doi:10.4018/979-8-3693-9641-4.ch007.
57. Mulani AO, Liyakat KKS, Warade NS, Patil A, Kolte MT, Kinage K, et al. ML-powered Internet of Medical Things structure for heart disease prediction. J Pharmacol Pharmacother. 2025. doi:10.1177/0976500X241306184.
58. Odnala S, Shanthy R, Bharathi B, Pandey C, Rachapalli A, Liyakat KKS. Artificial intelligence and cloud-enabled E-vehicle design with wireless sensor integration. SSRN Electron J. 2025. doi:10.2139/ssrn.5107242.

59. Neeraja P, Kumar RG, Kumar MS, Liyakat KKS, Vani MS. DL-based somnolence detection for improved driver safety and alertness monitoring. 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India. 2024. p. 589–94. doi:10.1109/IC2PCT60090.2024.10486714.
60. Magadum PK. Machine learning for predicting wind turbine output power in wind energy conversion systems. Grenze Int J Eng Technol. 2024;10:2074–80. Available from: https://thegrenze.com/index.php?display=page&view=journalabstract&absid=2514&id=8
61. Nerkar PM, Dhaware BU. Predictive data analytics framework based on Heart Healthcare System (HHS) using machine learning. J Adv Zool. 2023;44(Special Issue 2):3673–86. Available from: https://jazindia.com/index.php/jaz/article/view/1695
62. Nerkar P, Sultanabanu. IoT-based skin health monitoring system. Int J Biol Pharm Allied Sci. 2024;13:5937–50. doi:10.31032/IJBPAS/2024/13.11.8488.
63. Kazi KSL, Khadake SB, Chounde AB, Suryagan AA, Khadatare MR. AI-driven-IoT (AIIoT) based decision making system for high-blood pressure patient healthcare monitoring. 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India. p. 96–102. doi:10.1109/ICSCNA63714.2024.10863954.
64. Kazi KSL. AI-powered-IoT (AIIoT)-based decision-making system for BP patient's healthcare monitoring: KSK approach for BP patient healthcare monitoring. In: Aouadni S, Aouadni I, editors. Recent Theories and Applications for Multicriteria Decision-Making. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 205–38. doi:10.4018/979-8-3693-6502-1.ch008.
65. Kazi KSL. AI-powered IoT (AI IoT) for decision-making in smart agriculture: KSK approach for smart agriculture. In: Hai-Jew S, editor. Enhancing Automated Decision-Making Through AI. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 67–96. doi:10.4018/979-8-3693-6230-3.ch003.
66. Kazi KSL. KK approach to increase resilience in Internet of Things: A T-cell security concept. In: Darwish D, Charan K, editors. Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 87–120. doi:10.4018/979-8-3693-9491-5.ch005.
67. Kazi KSL. KK approach for IoT security: T-cell concept. In: Kumar R, Peng S-L, Jain P, Elngar AA, editors. Deep Learning Innovations for Securing Critical Infrastructures. Hershey (PA): IGI Global Scientific Publishing; 2025. p. 369-90. doi: 10.4018/979-8-3373-0563-9.ch022.
68. Kazi KSL. Healthcare monitoring system driven by machine learning and Internet of Medical Things (MLIoMT). In: Kumar VV, Katina PF, Zhao J, editors. Convergence of Internet of Medical Things (IoMT) and Generative AI. Hershey, PA: IGI Global Scientific Publishing; 2025. p. 385–416. doi:10.4018/979-8-3693-6180-1.ch016.
69. Kazi KSL, Shinde SS, Nerkar PM, Kazi SS, Kazi VS. Machine learning for brand protection: A review of a proactive defense mechanism. In: Khan MI, Haq MAU, editors. Avoiding Ad Fraud and Supporting Brand Safety: Programmatic Advertising Solutions. Hershey, PA: IGI Global Scientific Publishing; 2025. p. 175–220. doi:10.4018/979-8-3693-7041-4.ch007.
70. Upadhyaya AN, Surekha C, Malathi P, Suresh G, Suriyan K, Liyakat KKS. Pioneering cognitive computing for transformative healthcare innovations. SSRN Electron J. 2025. doi:10.2139/ssrn.5086894.

