STM JOURNALS

Journal of
VLSI Design Tools & Technology

ISSN: 2249-474X (Online)
ISSN: 2321-6492 (Print)
Volume 15, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoVDTT

https://journals.stmjournals.com/jovdtt

Review JoVDTT

IoT Network Security Employing KVS Approach: Novel Approach to IoT Security with B-Cell Inspired Models Implemented using Artificial Intelligence

Nikat Rajak Mulla[1,*], Kazi Kutubuddin Sayyad Liyakat[2]

Abstract

The Internet of Things (IoT), which links billions of devices that gather, analyse, and send data, is growing quickly. Although there are many benefits to this interconnection, there are also serious security risks. Conventional security measures frequently struggle to keep up with the dynamic and diverse nature of IoT environments. Innovative security ideas are being investigated in response, and the B-Cell concept, also known as the Kutubuddin Vahida Sultana (KVS) approach for IoT security, is one promising strategy. B-cells are an essential part of the adaptive immune system in immunology. As they go throughout the body, they identify antigens, or foreign chemicals, and create antibodies that are specifically designed to counteract those dangers. Inspired by the human immune system, the B-Cell idea presents a fresh approach to protecting IoT networks and devices. The B-Cell concept, which is applied by artificial intelligence, attempts to provide IoT devices with the capacity to learn, adapt, and defend against changing cyberattacks, much like B-cells in our bodies learn to identify and eliminate dangers. With billions of gadgets linking our homes, communities, and industries, the Internet of Things is rapidly expanding. But this quick growth has revealed a serious weakness: security. The absence of strong security in IoT devices is a serious risk, as it may lead to everything from industrial control systems being taken over to smart refrigerators spying on us. This IoT nature has prompted academics to investigate non-traditional methods, such as taking cues from the amazing immune system, particularly the B-cell theory. We recommend checking the accuracy and response time of networks using the Kutubuddin Vahida Sultana (KVS) Approach. The response of the proposed KVS Approach has better precision as compared to the present approaches.

Keywords: IoT security, KVS approach, B-cell, cybersecurity, cyberattacks, IoT threats, artificial intelligence

INTRODUCTION

The Internet of Things (IoT), which connects billions of objects and is revolutionizing sectors, is growing rapidly. But there are also significant security challenges brought forth by the interconnection. Malicious actors target IoT devices because they are often resource-constrained and lack strong security features. The dynamic threat landscape makes it difficult for traditional security measures to keep up, necessitating creative solutions. This study examines an intriguing strategy for addressing IoT security: taking cues from the human body's amazing immune system, particularly the complex defence mechanisms of B-cells.

The vulnerabilities in IoT devices are multifaceted. They include:

***Author for Correspondence**
Nikat Rajak Mulla
E-mail: nikatmulla786@gmail.com

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

Received Date: May 27, 2025
Accepted Date: August 05, 2025
Published Date: December 13, 2025

Citation: Nikat Rajak Mulla, Kazi Kutubuddin Sayyad Liyakat. IoT Network Security Employing KVS Approach: Novel Approach to IoT Security with B-Cell Inspired Models Implemented using Artificial Intelligence. Journal of VLSI Design Tools & Technology. 2025; 15(3): 36-46p.

- *Limited Processing Power and Memory:* Makes implementing complex security algorithms difficult.
- *Lack of Regular Updates:* Leaves devices exposed to known vulnerabilities.
- *Default Passwords:* Easily exploited by attackers.
- *Insecure Communication Protocols:* Susceptible to eavesdropping and manipulation.
- *Diverse Device Ecosystem:* Makes standardization and widespread security patches challenging.

A favourable environment for cyberattacks is produced by this confluence of elements, which can result in data breaches, network outages, and even bodily injury. When it comes to new and quickly changing IoT threats, traditional security solutions that mostly depend on static signatures and recognised threat patterns are sometimes unsuccessful [1-5].

The immune system of the human body offers a convincing example of strong and flexible security. It has developed over thousands of years to protect against an ever-increasing number of infections. The B-cell, one of its essential parts, provides an especially intriguing comparison for IoT security.

The lymphocyte type that produces antibodies is called a B-cell. This is how they operate:

- *Antigen Recognition:* Each B-cell has an exclusive receptor on its surface, which may bind to a definite antigen (a foreign substance).
- *Activation and Clonal Selection:* When a B-cell meets its corresponding antigen, it is activated and experiences clonal selection, meaning it rapidly multiplies, creating a large population of B-cells with the same receptor.
- *Antibody Production:* These cloned B-cells differentiate into plasma cells that produce and discharge large quantities of antibodies that bind to antigen, neutralizing or patterning it for obliteration.
- *Memory Cells:* Some activated B-cells differentiate into memory cells. These long-lived cells provide immunological memory. If the same antigen is encountered again, the memory cells respond much faster and more effectively, providing rapid protection.

The adaptive and distributed nature of the B-cell response can be translated into effective IoT security strategies. Here is how:

- *Device Behaviour Anomaly Detection:* Imagine each IoT device as a B-cell with a unique receptor "trained" to recognize normal device behaviour (e.g., data transmission patterns, resource usage). Anomalous behaviour, triggered by malicious code or compromised functionality, would act as an "antigen".
- *Adaptive Security Policies:* Just as B-cells respond to specific antigens, security policies can be dynamically adjusted based on detected anomalies. For example, if unusual network traffic is detected on a particular device, the system could automatically isolate the device, tighten firewall rules, or trigger a security audit.
- *Distributed Security Intelligence:* A network of IoT security agents, each mimicking a B-cell, could collectively monitor the IoT environment. If an agent detects suspicious activity, it can "alert" neighbouring agents, triggering a coordinated response. This distributed approach enhances resilience and avoids single points of failure.
- *"Memory Cell" for Learned Threats:* Information about detected threats and successful defences can be stored and used to improve future responses, analogous to the memory function of B-cells. This ensures the system learns and adapts to the evolving threat landscape.

Benefits of a B-Cell-Inspired IoT Security Model

- *Adaptability:* The system can adapt to new and unforeseen threats without requiring pre-programmed signatures.
- *Distributed Protection:* The distributed nature of the approach enhances resilience and reduces the impact of individual device compromise.
- *Scalability:* The model can be scaled to accommodate the growing number of IoT devices.
- *Resource Efficiency:* The algorithms can be optimized to operate on resource-constrained devices.

Researchers are actively exploring various implementations of B-cell-inspired models for IoT security. These include:

- *Artificial Immune Systems (AIS):* Developing algorithms that mimic the key functions of the immune system, including B-cell antibody production and clonal selection.
- *Machine Learning:* Using ML techniques to train simulations that can recognize and respond to anomalous device behaviour.
- *Blockchain Technology:* Leveraging blockchain to securely store and share threat intelligence among IoT devices and security agents.

Security solutions that are both inventive and adaptable are required because of the growing complexity and scale of the Internet of Things landscape. A method that seems promising is one that takes its cues from the human immune system, namely the idea of B-cells. Through the process of imitating the adaptive, dispersed, and learning characteristics of B-cells, we are able to construct Internet of Things security solutions that are more robust and resilient, hence providing effective protection against increasing cyber threats. Despite the fact that it is still in its early phases, this bio-inspired approach has the potential to revolutionise the way we protect the Internet of Things, thereby assuring a safer and more reliable connected future [6-15].

B-CELL IN THE HUMAN BODY: A MODEL FOR A SMARTER IOT SECURITY

While IoT holds the promise of a linked future, it also poses serious security issues. Traditional security measures are insufficient due to the sheer number of devices, the variety of functionality within those devices, and the frequently restricted computing capability of those devices. We require a security approach that is both more flexible and more long-lasting. The human body, and more specifically its B-cells, can serve as a source of inspiration for a novel approach to IoT security, which we call as KVS (Kutubuddin Vahida Sultana) Approach. It is interesting to note that nature provides a compelling model [16-22].

The B-cells that make up our adaptive immune system are an essential component. They are continuously coming into contact with antigens, which are foreign invaders such as germs and viruses, as they patrol our bodies. A fascinating procedure takes place in a B-cell when it recognises an antigen, which is as follows:

- *Recognition:* Each B-cell has a unique antibody that can bind to a specific antigen. This recognition triggers an immune response.
- *Clonal Expansion:* The B-cell that recognizes the antigen rapidly multiplies, creating a larger force to combat the specific threat.
- *Affinity Maturation:* These newly replicated B-cells refine their antibodies, becoming even more effective at targeting the antigen.
- *Memory Cells:* A subset of these B-cells develops memory cells, giving long-term immunity against future encounters with the same antigen.

This dynamic process allows the human body to learn, adapt, and defend itself against a constantly evolving landscape of threats. Can we translate this biological mechanism into a better security framework for IoT?

Imagine each IoT device as having its own virtual "B-cell" system. This system would operate in the following manner:

1. *Anomaly Detection as Antigen Recognition:* Instead of antigens, the "B-cell" monitors the device's behaviour for anomalies like unusual network traffic, unexpected data outputs, or unauthorized access attempts. These anomalies are analogous to foreign invaders.
2. *Pattern Recognition and Threat Signature Generation:* When an anomaly is detected, the system analyses it to identify patterns and generate a threat signature, much like a B-cell developing an antibody [11-15].
3. *Local Mitigation and Response:* The device then takes immediate action to mitigate the threat, such as blocking suspicious connections or isolating compromised components. This is equivalent to the B-cell neutralizing the antigen directly.

4. *Network-Wide Knowledge Sharing (Clonal Expansion and Affinity Maturation):* The crucial element here is that learned threat signatures are shared across the network of IoT devices. When one device detects a threat, it "alerts" its neighbours. These neighbours then use this information to proactively monitor for the same threat pattern, effectively creating a "clonal expansion" of security. Furthermore, sharing data about successful mitigation strategies allows the network to refine its defences, mimicking "affinity maturation".
5. *Memory and Predictive Security:* The system retains information about past threats and vulnerabilities, building a knowledge base for future defence, analogous to the B-cell's memory cells. This allows the system to anticipate and proactively defend against known threat patterns.

Benefits of a B-Cell-Inspired IoT Security Model

- *Adaptability:* Responds dynamically to new and evolving threats, unlike static security measures.
- *Distributed Intelligence:* Leverages the collective intelligence of the IoT network, creating a more resilient and robust defence.
- *Scalability:* Designed to handle the massive scale of IoT devices, as each device contributes to the overall security posture.
- *Reduced Reliance on Centralized Security:* Distributes security responsibilities, minimizing the risk of a single point of failure.
- *Proactive Security:* Shifts the focus from reactive response to proactive threat detection and prevention.

Challenges

While highly promising, implementing a B-cell-inspired IoT security model presents several challenges:

- *Resource Constraints:* Numerous IoT devices have limited handling power and memory. B-cell algorithm needs to be lightweight and efficient.
- *Data Privacy:* Sharing threat data across the network must be done securely and anonymously to protect user privacy [23-29].
- *Trust and Authentication:* Ensuring the authenticity and integrity of shared threat data is crucial to preventing malicious actors from poisoning the network.
- *Implementation Complexity:* Developing and deploying such a complex system requires significant engineering effort.

When it comes to safeguarding the increasingly complex and linked world of IoT, the security model that is inspired by B cells provides a compelling and unique solution. We are able to develop a security framework that is more robust, intelligent, and scalable if we model it after the adaptive defence mechanisms that are found in the human immune system. In spite of the fact that there are still obstacles to overcome, this strategy has the potential to bring about enormous benefits, opening the way for a future in which IoT devices are not only linked but also fundamentally safe. With the help of nature as a source of inspiration, we may construct a defence that is stronger and adaptable to the cyber threats that will emerge in the future. To the same extent that our bodies are continually changing in order to combat new diseases, our IoT security systems need to be able to adapt in order to defend us from the ever-evolving landscape of cyberthreats [29–33].

PROPOSED KVS APPROACH

IoT has become a pervasive technology that is reshaping the way we work and live. On the other hand, the prevalence of cyberattacks increases in tandem with the number of IoT devices. Utilising B-cell ideas is one method that can be utilised to enhance the security of IoT. B-cells, which are an essential part of the human immune system, have the potential to play a role in the development of a new generation of security systems that are able to identify and respond to threats in real time. The stages that are involved in building a B-cell concept for IoT security have been discussed in this study. Kutubuddin Vahida Sultana is the name of the method that is labelled on the inventor's family members' names: Kutubuddin, which means "brother", Vahida, and Sultanabanu, which means "sisters" (Figure 1).

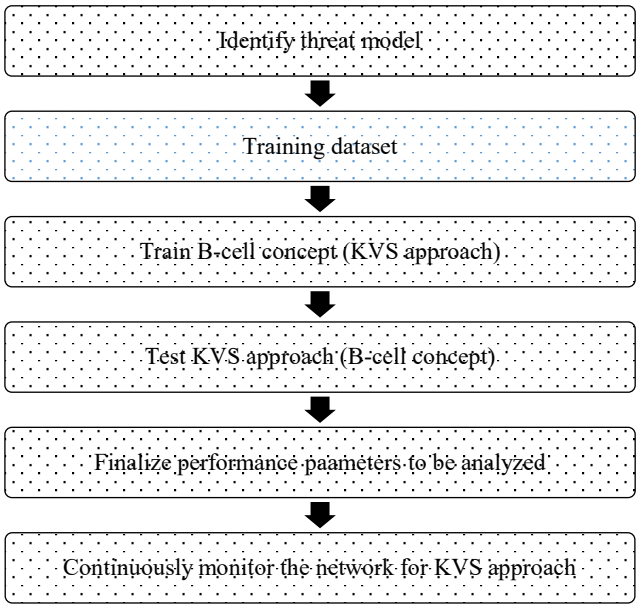

Figure 1. Proposed KVS approach.

Step 1: Identify the Threat Model

The first step in designing a B-cell concept for IoT security is to identify the threat model. This involves analysing the potential threats that the IoT system may face and identifying the vulnerabilities that could be exploited. It is essential to consider all possible attack vectors, including physical, network, and application-level attacks. Once the threat model has been identified, it is possible to design a security system that can detect and respond to these threats effectively.

Step 2: Develop a Training Dataset

The next step is to develop a training dataset that can be used to train the B-cell concept. The training dataset should include examples of both normal and abnormal behaviour, so the B-cell concept can learn to distinguish between them. It is essential to safeguard that the training dataset is evocative of the real-world environment in which the B-cell concept will be deployed. This will help ensure that the B-cell concept is effective in detecting and responding to threats.

Step 3: Train the B-Cell Concept

Once the training dataset has been developed, it is time to train the B-cell concept. This involves using machine learning algorithms to analyse the training dataset and identify patterns of behaviour that are associated with normal and abnormal behaviour. The B-cell concept should be trained to detect even subtle changes in behaviour, as these could indicate a potential threat. It is essential to ensure that the B-cell concept is trained using a large and diverse dataset, as this will help ensure that it can detect a wide range of threats.

Step 4: Test the B-Cell Concept

After the B-cell concept has been trained, it is time to test it to ensure that it can detect and respond to threats effectively. This involves exposing the B-cell concept to a range of different threats and measuring its performance. It is essential to ensure that the B-cell concept can detect threats accurately and quickly, as this will help minimize the impact of a cyberattack.

Step 5: Deploy the B-Cell Concept

Once the B-cell concept has been tested and validated, it is time to deploy it in the real-world environment. This involves integrating the B-cell concept into the existing IoT system and configuring it to detect and react to threats in real-time. It is essential to ensure that the B-cell concept is deployed securely and that it is protected from potential attacks.

Step 6: Monitor and Update the B-Cell Concept

After the B-cell concept has been deployed, it is essential to monitor its performance and update it regularly. This involves analysing the data collected by the B-cell concept and using it to improve its performance over time. It is also essential to ensure that the B-cell concept is updated regularly to reflect changes in the threat landscape.

Creating a B-cell idea for IoT security is a complicated procedure that requires a number of steps to be completed. It is possible to develop a B-cell idea that is capable of detecting and reacting to threats in real time by following the methods that are explained in this study. This would contribute to the improvement of the security of IoT systems. It is conceivable to construct a new generation of security systems that are able to react to changing threats and assist in protecting IoT systems from cyberattacks by utilising B-cell concepts.

DISCUSSION

The core idea is to translate the principles of B-cell behaviour into algorithms and protocols that enhance the security of IoT devices. How might this work in practice?

1. *Defining "Antigens" in the IoT World:* First, we need to define what constitutes a "threat" or "antigen" in the context of IoT. This could include malicious code, unauthorized access attempts, anomalous network traffic patterns, or deviations from expected device behaviour.
2. *Creating Digital Antibodies:* Algorithms would be designed to detect and respond to these defined threats. These "digital antibodies" could take the form of:
    - *Signature-based detection:* Similar to how antibodies bind to specific antigens, these algorithms identify known malicious patterns.
    - *Anomaly detection:* These algorithms learn the normal behaviour of a device and flag deviations as potential threats.
    - *Rule-based filtering:* Defining rules based on known vulnerabilities and attack vectors to block malicious activity.
3. *Adaptive Learning and Memory:* Perhaps the most compelling aspect of B-cell-inspired security is its potential for adaptability. ML algorithms may be used to mimic the "learning" process of the immune system. When a new threat is detected, the system can analyse it, develop a response, and "remember" this response for future encounters. This could involve:
    - *Generating new rules:* Automatically creating new rules to block similar attacks.
    - *Updating existing signatures:* Adapting signatures to account for variations in malicious code.
    - *Sharing threat intelligence:* Distributing information about new threats across a network of IoT devices, enabling a collective defence.
4. *Distributed Security Architecture:* Just as B-cells operate in a decentralized manner, the security system could be distributed across the IoT network. Each device (or a cluster of devices) could act like a "node" in the immune system, responsible for monitoring its local environment, detecting threats, and sharing information with other nodes.

Challenges

The concept of applying B-cell principles to IoT security is promising, but several challenges must be addressed:

- *Computational Constraints:* IoT devices frequently have inadequate processing power and memory. Developing complex algorithms that can run efficiently on these devices is a significant challenge.
- *Data Heterogeneity:* IoT devices generate diverse types of data, making it difficult to develop a unified threat detection system.
- *Privacy Concerns:* Collecting and analysing data for threat detection can raise privacy concerns. Implementing privacy-preserving techniques is crucial.
- *Scalability:* The IoT is a rapidly growing ecosystem. The security system must be able to scale to accommodate billions of devices.

- *False Positives:* Anomaly detection algorithms can sometimes generate false positives, flagging legitimate behaviour as suspicious. Minimizing false positives is essential to avoid disrupting normal operations.

Benefits

Despite these challenges, the potential benefits of B-cell-inspired IoT security are significant:

- *Enhanced Threat Detection:* The adaptive nature of the system can improve the ability to detect new and unknown threats.
- *Improved Resilience:* A distributed security architecture can make the system more resilient to attacks.
- *Reduced Reliance on Centralized Security:* The decentralized nature of the system can reduce the reliance on centralized security servers, which can be a single point of failure.
- *Autonomous Security:* The system can potentially operate autonomously, reducing the need for human intervention.

There is no silver bullet when it comes to improving the security of IoT devices; yet, B-cell-inspired security indicates a potential trend in this regard. Researchers have the ability to design security solutions that are more robust, adaptive, and resilient by pulling inspiration from the natural world. These solutions can ultimately assist in protecting the increasingly linked world in which we live. For the purpose of overcoming the challenges and fully appreciating the potential of this novel technique, additional study and expansion are required. It is possible that the future of a safe IoT will involve imitating the clever defence systems that have been designed over the course of millions of years of evolution.

The Steps of the B-cell Concept, as Applied to the Context of IoT Security

The B-cell concept, as applied to the context of IoT security, often entails the following steps:

1. *Antigen Recognition:* The "antigens" are characteristics of network traffic or device behaviour that can indicate malicious activity. This could include unusual data patterns, communication frequency, resource consumption, or deviations from expected functionality.
2. *Artificial B-Cells:* These are software agents deployed within the IoT network, each equipped with a unique "receptor" or detection rule. These rules are often based on machine learning algorithms trained on both benign and malicious data.
3. *Matching and Activation:* When an artificial B-cell detects a potential "antigen" (suspicious activity), it gets “activated”. This triggers further analysis and potentially initiates a response.
4. *Proliferation and Adaptation:* Activated B-cells can "proliferate" by creating additional copies of themselves to handle the detected threat. They can also "adapt" their detection rules based on the new attack patterns observed, enhancing their future effectiveness.
5. *Response:* Depending on the severity and nature of the threat, the B-cell system can initiate various responses, such as isolating the malicious node, blocking its communication, or alerting network administrators.

Advantages of the B-cell Concept

The B-cell concept offers several potential advantages over traditional security methods:

- *Adaptive and Proactive:* Unlike signature-based systems, B-cell systems can learn and adapt to new and evolving threats, making them more robust against zero-day attacks.
- *Distributed Detection:* The distributed nature of artificial B-cells allows for localized detection and response, minimizing latency and preventing widespread damage.
- *Anomaly Detection:* By learning normal device behaviour, B-cells can identify anomalies that may indicate malicious activity, even if the specific attack pattern is unknown.
- *Scalability:* The B-cell approach can be scaled to accommodate large and complex IoT networks by deploying more artificial B-cells as needed.

The B-cell Concept Challenges

Despite its promise, the B-cell concept for IoT security faces several challenges:

- *Computational Overhead:* Training and deploying artificial B-cells can require significant computational resources, which may be a constraint in resource-constrained IoT devices.
- *False Positives:* Like any anomaly detection system, B-cell systems can generate false positives, leading to unnecessary isolation or blocking of legitimate devices.
- *Complexity:* Designing and implementing an effective B-cell system requires expertise in machine learning, network security, and IoT device characteristics.
- *Data Requirements:* Training the B-cell system requires a large and representative dataset of both benign and malicious data, which can be difficult to obtain in practice.
- *Resource Constraints:* Deploying a full-fledged B-cell system on resource-constrained IoT devices presents a challenge. Lightweight algorithms and optimized implementations are crucial.

PERFORMANCE PARAMETERS FOR KVS APPROACH IOT SECURITY SYSTEMS

A B-cell-inspired IoT security system can be evaluated based on several key parameters:

- *Detection Accuracy:* This is arguably the most crucial parameter. It measures the system's ability to correctly identify anomalies (malicious activities) while minimizing false positives. High detection accuracy ensures that real threats are caught without disrupting normal operations. Metrics like *True Positive Rate (TPR - Sensitivity)* and *False Positive Rate (FPR - Specificity)* are commonly used to assess this. A good system aims for high TPR and low FPR.
- *False Alarm Rate (FAR):* A high FAR can render the system unusable. IoT environments often generate a lot of noise, and misclassifying normal fluctuations as attacks can lead to system administrators ignoring alerts or deactivating the security mechanism. A low FAR is critical for maintaining trust in the system.
- *Training Time:* The time required to train the B-cell-inspired system on normal data is a crucial factor, especially in dynamic IoT environments where normal behaviour can evolve over time. Shorter training times allow for faster deployment and adaptation to changing network conditions. This is particularly important for resource-constrained IoT devices.
- *Response Time:* Once an anomaly is detected, the system's response time is critical in limiting the damage caused by the attack. This includes the time taken to analyse the anomaly, identify the type of attack, and initiate appropriate mitigation measures. A short response time is crucial in preventing widespread damage.
- *Resource Consumption:* IoT devices are often resource-constrained, with limited processing power, memory, and battery life. The B-cell-inspired algorithm must be lightweight and require minimal resources to operate effectively on these devices. Metrics like CPU utilization, memory footprint, and energy consumption are important considerations.
- *Adaptability:* IoT environments are dynamic, and network behaviour can change over time due to software updates, new device deployments, or evolving user behaviour. A robust B-cell-inspired system should be able to adapt to these changes and maintain high detection accuracy without requiring frequent retraining.
- *Scalability:* IoT networks can be vast and complex, comprising thousands or even millions of devices. The B-cell-inspired algorithm should be scalable to handle the large volume of data generated by these networks without compromising performance.

Several factors can influence the performance of a B-cell-inspired IoT security system, including:

- *Feature Selection:* Choosing the right features to represent network behaviour is crucial for accurate anomaly detection. Relevant features might include network traffic volume, packet size, connection duration, and the frequency of specific events.
- *Data Preprocessing:* Cleaning and preprocessing the data before training the B-cell-inspired system is essential to remove noise and outliers that can negatively impact performance.
- *Algorithm Parameters:* Parameters like the number of B-cells, the affinity threshold, and the mutation rate can significantly impact the algorithm's performance. Careful tuning of these parameters is necessary to achieve optimal results.
- *Dataset Quality:* The quality and representativeness of the training data are crucial for building a robust and accurate system. The training data should accurately reflect the normal behaviour of the IoT network.

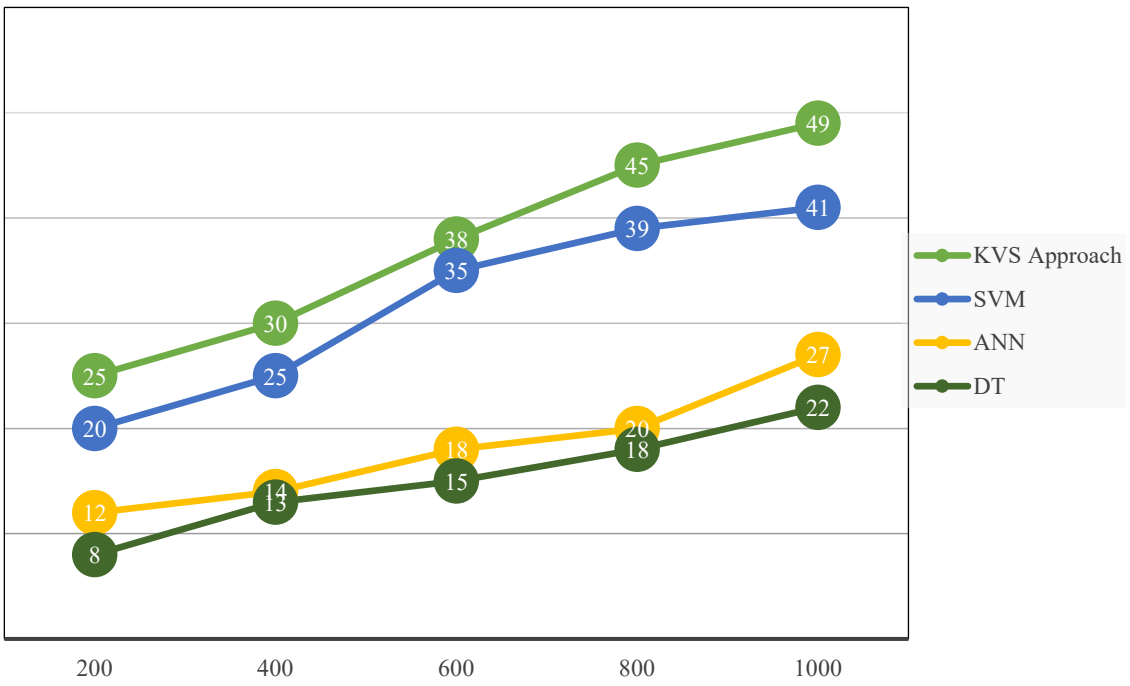

Figure 2. Precision comparison between KVS, SVM, ANN, and DT approaches.

Abnormality detection that is inspired by B cells is a promising technology that has the potential to improve the security of IoT ecosystems. The adaptive immune system is modelled after these algorithms, which allow it to efficiently recognise and respond to threats that are constantly evolving. Regarding the design and implementation of efficient B-cell-based IoT security systems, however, it is essential to give careful consideration to the performance parameters that were addressed earlier. It is necessary to continue research and development in order to optimise these algorithms for the specific problems that are presented by IoT environments and to guarantee that they are able to offer security solutions that are both strong and lightweight for the ever-expanding universe of connected devices. Within the framework of the Kutubuddin Vahida Sultana (KVS) strategy, we recommend examining the accuracy and response time of the networks. The comparison of precision for the proposed KVS approach with other presented SVM, ANN, and DT approaches is shown in Figure 2.

CONCLUSION

In terms of the future of IoT security, the B-Cell concept presents an intriguing prospect. IoT devices will be equipped with the ability to learn, adapt, and protect themselves against developing cyberattacks if this strategy is implemented. The idea for this approach comes from the human immune system. The initiatives are paving the way for the general adoption of this unique security paradigm, despite the fact that there are still difficulties to overcome. It is possible that the B-Cell concept will prove to be an essential defence mechanism against the increasingly complex threats that are posed to connected devices as IoT continues to grow. The concept of the B-cell is a viable method for improving the security of IoT networks by providing capabilities for anomaly-based detection, distributed detection, and adaptive detection. These efficient B-cell systems have the potential to assist in immunising IoT networks against the ever-changing landscape of cyber threats. In order to guarantee IoT's dependability and safety as it continues to expand, it will be necessary to implement cutting-edge security solutions such as the B-cell idea. Although the buzz is warranted, additional refining is required in order to firmly establish the B-cell strategy as an essential component of IoT security. Within the framework of the Kutubuddin Vahida Sultana (KVS) strategy, we recommend examining the accuracy and response time of the networks. The Precision of the proposed KVS approach is shown in Figure 2 and is better than the present IoT security methods.

REFERENCES

1. Kazi KS. KK approach to increase resilience in Internet of Things: A T-cell security concept. In: Almaiah M, Salloum S, editors. Cryptography, Biometrics, and Anonymity in Cybersecurity Management. Pennsylvania (USA): IGI Global; 2025. p. 199–228. doi:10.4018/979-8-3693-8014-7.ch010
2. Sayyad. 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. Pennsylvania (USA): IGI Global; 2025. p. 87–120. doi:10.4018/979-8-3693-9491-5.ch005
3. Khadake S, Kawade S, Moholkar S, Pawar M. A review of 6G technologies and its advantages over 5G technology. In: Pawar PM, et al., editors. Techno-Societal 2022 (ICATSA 2022). Cham: Springer; 2024. p. 107. doi:10.1007/978-3-031-34644-6_107
4. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, et al. Review of AI in power electronics and drive systems. In: Proc 3rd Int Conf Power Electron IoT Appl Renew Energy Control (PARC); 2024; Mathura, India. p. 94–99. doi:10.1109/PARC59193.2024.10486488
5. Dudgikar AB, Ingalgi AA, Jamadar AG, Swami OR, Khadake SB, et al. 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(1):204–8. doi:10.48175/IJARSCT-7867
6. Khadake SB, Patil VJ. Prototype design and development of solar-based electric vehicle. In: Proc 3rd Int Conf Smart Gen Comput Commun Netw (SMART GENCON); 2023; Bangalore, India. p. 1–7. doi:10.1109/SMARTGENCON60755.2023.10442455
7. Patil VJ, Khadake SB, Tamboli DA, Mallad HM, Takpere SM, et al. A comprehensive analysis of artificial intelligence integration in electrical engineering. In: Proc 5th Int Conf Mobile Comput Sustain Inform (ICMCSI); 2024; Lalitpur, Nepal. 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 current vehicle travel data. JNX. 2021 Jan;1–4.
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(2):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(2):362–7. doi:10.48175/IJARSCT-11364
11. Landage SS, Chavan SR, Kokate PA, Lohar SP, Pawar MK, et al. Solar outdoor air purifier with air quality monitoring system. In: Proc NCSTEM 2023. 2024. p. 260–6.
12. Khadake SB. Detecting salient objects of natural scene in a video using spatio-temporal saliency and colour map. JNX. 2021;2(8):30–5.
13. Khadake SB. Detecting salient objects in a video using spatio-temporal saliency and colour map. Int J Innov Eng Res Technol. 2021;3(8):1–9.
14. Bhosale PS, Kokare PD, Potdar DS, Waghmode SD, Sawant VA, et al. DTMF-based irrigation water pump control system. In: Proc NCSTEM 2023. 2024. p. 267–73.
15. Korake P, Murade H, Doke R, Narale V, Khadake SB, et al. Automatic load sharing of distribution transformer using PLC. In: Proc NCSTEM 2023. 2024. p. 253–9.
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(2):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. In: Proc 15th Int Conf Adv Comput Control Telecommun Technol (ACT); 2024. Vol 2. p. 5487–94.
18. Khadake SB, Patil VJ, Mallad HM, Gopnarayan BB, Patil KB. Maximize farming productivity through Agriculture 4.0-based intelligence using Agri-Tech Sense system. In: Proc ACT 2024. 2024. Vol 2. p. 5127–34.

19. Khedekar SV, Kawade AM, Vyavahare SS, Kashid PJ, Chounde AB, et al. Solar-based electric vehicle charging system – review. Int J Adv Res Sci Commun Technol. 2024;4(2):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(3):225–40. doi:10.48175/IJARSCT-22836
21. Veena C, Sridevi M, Liyakat KKS, Saha B, Reddy SR, et al. HEECCNB: an efficient IoT-cloud architecture for secure patient data transmission. In: Proc 7th Int Conf Image Inf Process (ICIIP); 2023. p. 407–10. doi:10.1109/ICIIP61524.2023.10537627
22. Kazi S. Computer-aided diagnosis in ophthalmology: a technical review of deep learning applications. In: Garcia M, de Almeida R, editors. Transformative Approaches to Patient Literacy and Healthcare Innovation. Pennsylvania (USA): IGI Global; 2024. p. 112–35. doi:10.4018/979-8-3693-3661-8.ch006
23. Liyakat KKS. AI-driven IoT-based decision making in kidney disease patient healthcare monitoring. In: Polat LÖ, Polat O, editors. AI-Driven Innovation in Healthcare Data Analytics. Pennsylvania (USA): IGI Global; 2025. p. 277–306. doi:10.4018/979-8-3693-7277-7.ch009
24. Pradeepa M, et al. Student health detection using machine learning and IoT. In: Proc IEEE 2nd Mysore Sub-Section Int Conf (MysuruCon); 2022.
25. Mahant MA. Machine learning-driven Internet of Things-based healthcare monitoring system. In: Wickramasinghe N, editor. Digitalization and the Transformation of the Healthcare Sector. Pennsylvania (USA): IGI Global; 2025. p. 205–36. doi:10.4018/979-8-3693-9641-4.ch007
26. Mulani AO, Liyakat KKS, Warade NS, et al. ML-powered Internet of Medical Things structure for heart disease prediction. J Pharmacol Pharmacother. 2025;0(0). doi:10.1177/0976500X241306184
27. Odnala S, Shanthy R, Bharathi B, Pandey C, Rachapalli A, et al. Artificial intelligence and cloud-enabled e-vehicle design with wireless sensor integration. SSRN Electron J. 2025. doi:10.2139/ssrn.5107242
28. Neeraja P, Kumar RG, Kumar MS, Liyakat KKS, Vani MS. DL-based somnolence detection for improved driver safety. In: Proc IEEE Int Conf Comput Power Commun Technol (IC2PCT); 2024. p. 589–94. doi:10.1109/IC2PCT60090.2024.10486714
29. Nerkar PM, Dhaware BU. Predictive data analytics framework for heart healthcare using machine learning. J Adv Zool. 2023;44(Spl-2):3673–86.
30. Nerkar P, Sultanabanu. IoT-based skin health monitoring system. Int J Biol Pharm Allied Sci. 2024;13(11):5937–50. doi:10.31032/IJBPAS/2024/13.11.8488
31. Ravale P. FPGA-based finger vein recognition system for personal verification. Int J Eng Res Gen Sci. 2015;3(4):382–8.
32. Ravale PM, et al. Retinal image decomposition using variational mode decomposition. Int Res J Eng Technol. 2018;5(6):2510–12.
33. Silpa Raj M, Kumar RS, Jayakumar K, Gopila M, Kumar S. Scalable IoT-enabled intelligent solutions for smart grids. In: Kannadhasan S, et al., editors. Proc Int Conf Sustain Innov Comput Eng (ICSICE 2024). Dordrecht (NL): Atlantis Press; 2025. p. 1004–16. doi:10.2991/978-94-6463-718-2_85

