ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

A MULTI-BIT ERROR-TOLERANT SRAM-BASED TCAM FOR ADVANCED NETWORK PERFORMANCE

RANGA ASWITHA, *Research Associate, Dept of R &D,*
NEWZEN INFOTECH, HYDERABAD

ABSTRACT: Ternary content addressable memory (TCAM) is utilized for rapid data access. In the realm of TCAM production, ASICs have always been regarded as the benchmark of excellence. Nonetheless, a field-programmable gate array (FPGA) is employed in the fabrication of SRAM-based TCAMs. Data continues to be supplied through Content-Addressable Memory (CAM) notwithstanding the ambiguity around its precise location and identity. Binary is the most used CAM format due to its exclusive use of the digits 0 and 1. Ternary content-addressable memory (TCAM) is, in comparison, more intricate than content-addressable memory (CAM). Bit-wise storing of any value is indeed feasible. The implementation of FPGA technology in accelerated tasks entails the potential for minor errors. These deficiencies heighten the probability that this method will fail to yield the intended outcomes. This is due to the fact that SRAM-based TCAMs occasionally struggle to effectively seek for and rectify minor mistakes. Contemporary technology simplifies the error detection process by using a single parity bit for each word. This technique enables the detection and correction of single-bit errors. The proposed method emphasizes the importance of multiple bit upsets (MBUs) to enhance the MBU diagnosis and repair processes. Row, column, and diagonal parity may be beneficial for detecting multi-bit errors. Individuals are often cared to on a one-on-one basis. Errors are promptly rectified to maintain the efficacy of the search process.

Keywords: *Field-programmable gate array (FPGA), soft errors, static random access memory (SRAM)-based ternary content- addressable memory (TCAM).*

1. INTRODUCTION

The connection between the mind and brain, particularly regarding memory, exemplifies cognitive processes that are closely linked to neural activity in the brain. A range of valuable information, including maps and instructions, may be accessible on the platform. The subsequent events are elucidated by the recollections. A thorough examination from several perspectives is necessary for recall. The address range for each location or cell in a memory system commences at zero and extends to the memory capacity minus one. A data access memory can be categorized into one of four distinct types. Computer memory can be accessed through several methods, including arbitrary, sequential, content-addressable, direct, or random access (RAM, DAM, CAM, SAM). It is sometimes referred to as random-access memory, or RAM. Random Access Memory (RAM) data is susceptible to power interruptions. The inherent instability of the RAM is responsible for this. Static RAM (SRAM) and dynamic RAM (DRAM) are prevalent types of random access memory (RAM). During the operation, SAM is responsible for retrieving data from storage. Conversely, data can be accessed in any sequence via random access memory

ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

(RAM). Sequential access devices often accommodate both optical and magnetic media. The DAM home data has distinct physical components.

You will encounter no difficulties utilizing these instruments. Conversely, collecting all the necessary information regarding these names is straightforward and incurs no expense. Your most treasured life memories are concealed beneath a mysterious layer of magnetic sheets. Associative memory is often referred to as content-addressable memory (CAM). Specifically, BCAM and TCAM, representing binary and ternary content addressable memory, are the two types that are most frequently utilized.

The efficacy of a content-addressable memory (CAM) search relies on its ability to examine numerous data objects within a single cycle. Data is stored and accessed from binary content-addressable memory (CAM) utilizing a singular potential value. Network systems commonly utilize trinary content-addressable memory (TCAM) for the detection and filtration of transmission data. The 4x5 TCAM architecture depicted in Figure 1 is based on NOR logic and is straightforward. Address resolution relies on the capacity of a Content Addressable Memory (CAM) to maintain and modify the routing table. Certain TCAMs can exist in three distinct states: 0, 1, or x, the latter representing "do not care.

Four horizontal lines delineate the fundamental syllables of the CAM system. A single word can be encoded using merely five bits. Core cell channels facilitate the more efficient storage and comparison of information. Search information is extracted by Content-Addressable Memory (CAM) cells from the vertical search lines of the graphic. Each row in the array signifies a collection of search results, while the horizontal lines denote those results. Green lines indicate concordance of CAM words, whereas red lines signify discordance. The match lines inputted into the encoder include the names of the locations together with the match site.

Utilizing static random-access memory (SRAM), field programmable gate array (FPGA) technology rapidly fulfills the flexibility required for big data analytics, software-defined networking (SDN), and network accelerators. High-energy neutron particles can induce single-event interruptions (SEUs) in FPGA and SRAM-based circuits. One hypothesis posits that the proximity and small dimensions of memory cells in on-chip embedded memory influence the occurrence rate of SEUs. Following a single event upset (SEU) in embedded memory, data loss may arise from inadequate data management.

Interruptions varying from one bit to multiple bits may occur within the duration of a single event change. Cuckoo hashing is an effective and efficient method for rapidly generating binary content-addressed memory (CAMs) with field-programmable gate arrays (FPGAs). The effectiveness of the TCAM is typically determined by the block RAM (BRAM) and spread RAM (distRAM) of an SRAM-based FPGA. A false match or discrepancy may have resulted from a temporary glitch that caused the incorrect match address. The impacted SRAM word must be modified as a result of a minor error in order for queries to generate precise results. In TCAM systems that are based on SRAM, it is imperative to meticulously regulate search latency and efficacy.

ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

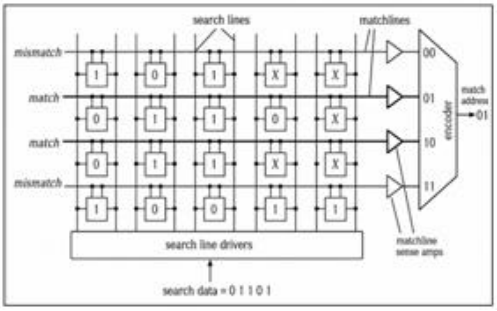

Fig. 1 TCAM (Ternary Content Addressable Memory) is a memory architecture.

This paper presents an efficient, rapid, and cost-effective method to safeguard SRAM-enabled TCAMs without compromising search efficacy. The proposed method enables the rapid and cost-effective identification and resolution of issues arising from multibit interruptions (MBUs). To detect multi-bit errors, three additional parity checks are employed alongside the conventional tests on rows, columns, and diagonals.

The elevated search rate is solely attributed to background automated error correction. The proposed method not only protects SRAM-enabled TCAMs in the current system but is also straightforward, cost-effective, and easy to install, while mitigating the adverse effects on search efficiency. Resolving issues need not need extensive time or computational resources when employing straightforward methods such as single-bit parity testing.

To rectify soft faults, the error-correction technique may utilize the supplementary binary-encoded TCAM database maintained for SRAM-based TCAM systems. Owing to its enhanced search functionalities, the error-correction system may operate continuously in the background, permitting other search processes to execute concurrently without disruption.

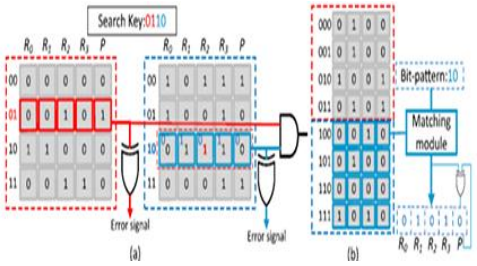

Fig. 2 ER-TCAMs are currently available and can be used to detect mistakes. These ER-TCAMs could potentially aid in error detection.

I sincerely apologize for any errors committed in the past.

Figure 2 illustrates the fundamental concept underlying the ER-TCAM methodology. The TCAM database ensures that matching data is consistently accessible, as it is kept in an 8-by-4 SRAM divided by two binary-encoded bits. Each word in Static Random Access Memory (SRAM) includes a parity bit that designates the Storage Buffer Unit (SBU). Figure 2(a) illustrates that this is guaranteed by Error-Resilient Ternary Content Addressable Memory (ER-TCAM). The lookups are finalized by verifying the accuracy of the read SRAM bits.

ER-TCAM utilizes supplementary data from the binary-encoded TCAM table to rectify misspelled words. Activating the search key 0110 on the SRAMs depicted in figure (a) will produce the binary representations of the phrases 00101 and 01110. In the second SRAM word, 011010, an SBU is generated if the parity and match bits deviate from the anticipated value. Figure 2a will exemplify this. Each TCAM element monitors binary data. As the data is stored as SRAM words, the ER-TCAM will have future access to it. The retrieved SRAM words yield the accurate bit pattern, which constitutes a component of the error-correction vector (ECV), together with the parity value (01010). The ECV was

ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

discovered to be compromised, resulting in overwriting of the SRAM word.

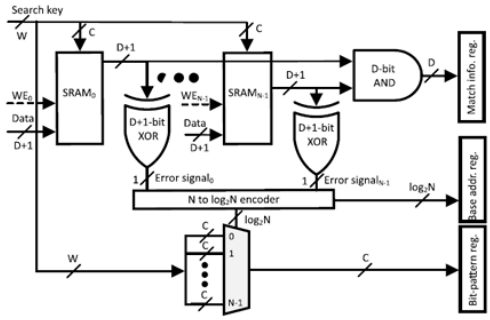

Fig. 3 Examine the issues that are currently plaguing the ER-TCAM configuration.

Figure 3 illustrates an erroneous ER-TCAM outcome. Upon activating the search key, the bits of the accessed SRAM words undergo an exclusive OR operation, resulting in the generation of the error signal. A log2N-bit error code is produced by the Ternary Content Addressable Memory (TCAM) when N Static Random Access Memories (SRAMs) detect improper data. Identifying security vulnerabilities in Static Random Access Memory (SRAM) technology is achievable with the previously provided code. The error repair technique entails gathering bit patterns of search keys and error codes.

This figure illustrates ER-TCAM technology, which denotes error-correcting tethered camera array. A unique type of random access memory (SRAM) is utilized to store the data of the TCAM table. The elements of static random access memory (SRAM) comprise a read/write driver, an ECV computing unit, and an address generating unit (AGU). The SRAM sub-block commences at the position indicated by the log2N bits of the SRAM ID, allowing the AGU to access all binary entries stored in the TCAM table.

The C-bit configuration of read TCAM words is utilized to acquire the parity and match bits during a D-clock cycle. The ECV comprises two bytes. In the event of a damaged SRAM word during read/write operations, the anticipated error correcting value (ECV) is utilized as a substitute. Subsequently, the appropriate SRAM will be activated by the high signal write enable. Note that SRAMs may require TCAMs to rectify errors occurring during retrieval processes, particularly in search activities. Consequently, the ER-TCAM offers advantages. The ER-TCAM converts SRAMs into dual-port RAM, enabling simultaneous reading and writing operations. The ER-TCAM's search operations and error correction mechanism operate concurrently, as the write port of the Static Random Access Memory (SRAM) includes the pre-computed Error Correction Vector (ECV). The binary-encoded table of ternary content-addressable memory (TCAM), which may contain soft errors, is stored in static random-access memory (SRAM). These issues arise, however they occur significantly less frequently in SRAMs with ternary content addressable memory compared to other types of SRAM.

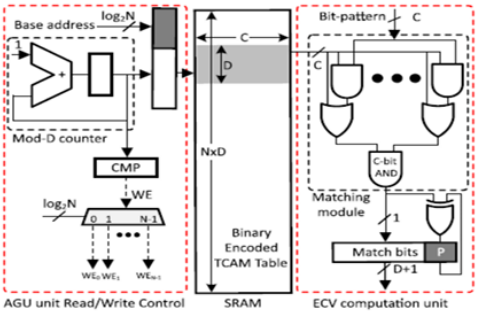

Fig. 4 Errors can now be corrected with the help of ER-TCAM.

2. TERNARY CONTENT ADDRESSABLE MEMORY

Network nodes frequently utilize TCAMs for the classification of data flows. Maintenance of security policies, delivery

ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

of data payloads, and software-defined networking (SDN) all depend on these components. This issue is particularly concerning as even little errors could alter data stored in memory. Should any issues be detected during the parity check, an error-correcting technique is employed to rectify them. Consequently, memory is preserved. An expanded vocabulary will be necessary for each phrase, which constitutes a disadvantage. This paper focuses on the memory safety of TCAM simulations. The objective of this methodology is to enhance the SRAM-Based TCAM Design by improving the reliability and speed of the error repair search mechanism while reducing the incidence of soft failures.

SRAM based TCAM on FPGAs

Contemporary field-programmable gate arrays (FPGAs) utilize ternary content-addressable memory (TCAM) technologies. The on-chip static random-access memory (SRAM) components supply the power for these systems. Whenever a 1 is inputted into RAM, the TCAM will transition to the 0 state [0]. Upon detecting a 1 in both SRAM[0] and SRAM[1], the TCAM transitions to the x state. Furthermore, a 1 in SRAM[1,] establishes the price as one. Constructing a C-bit TCAM design from a 1-bit SRAM often necessitates the utilization of 2C locations. It compares each word in the TCAM database to every potential C-bit code in the SRAM words to identify matches. A 2C-position SRAM can be constructed with a B-bit width to generate a TCAM featuring a C-bit wide B-word table. Scientists naturally differentiated between SRAM-based TCAMs, which necessitate greater memory, and TCAMs with larger bit patterns. A diverse array of methodologies for constructing TCAMs using FPGAs exists.

Error Detection and Correction in TCAM

There is a significant likelihood that several errors will be introduced by contemporary technology, particularly memory systems. The system may fail if any alteration occurs in a single byte of stored data. It is important to note that soft error rates on land are typically quite low. For instance, a projection indicated 109 bit errors annually for a 65 nm pitch static random-access memory (SRAM). In mission-critical systems such as communication networks, even a minor error rate can significantly affect performance, as components like routers must be dependable and readily accessible. Given the significance of software vulnerabilities, it is essential that network components, such as routers, be constructed with meticulous attention to prevent errors. Regularly employing error tests and repair codes may assist in identifying flaws that have been overlooked.

3. PROPOSED ERROR TOLERANT TCAM

The primary function of a ternary content-addressable memory device is to facilitate query execution. SRAM-based TCAMs utilize field-programmable gate arrays (FPGAs) to distinguish themselves from conventional TCAMs that depend on ASICs. Regardless of the file's designation or location, TCAM is an excellent instrument for data retrieval. Binary CAM, synonymous with TCAM, also indicates the data storage capacity. To incorporate numbers beyond zero and one, TCAM represents an enhanced iteration of CAM. If rapid systems utilizing FPGAs were to

ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

encounter soft errors, the technology would become entirely ineffective. Addressing minor issues in SRAM-based TCAMs can be challenging without significantly impeding research progress.

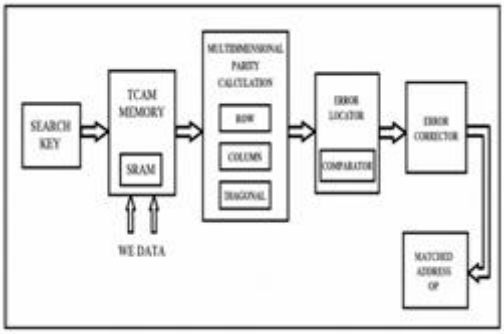

Fig.5 It is preferable to choose an approach that eliminates errors in TCAM blocks.

This research employed the single-bit disturbance identification and rectification method. Rectifying multiple bit disturbances (MBUs) is far more facile using this approach. The technique may identify errors in several bits by the use of row, column, and diagonal parity. A high search rate is facilitated by real-time background error correction. Figure 5 illustrates the block diagram of the proposed technique. To obtain the necessary pairings, the SRAM is instructed to activate the search key to locate analogous phrases. Immediate measures must be implemented upon the discovery of any discrepancies. Upon the identification of an error, the content is forwarded to the appropriate editing department for rectification. The revised version is subsequently stored in random access memory (RAM).

4. MULTIBIT UPSETS PROTECTION

Parity bits serve as a prevalent error-checking mechanism in microprocessors and are frequently integrated into each word of available memory. Each memory chip incorporates an error-checking function, enabling rapid and precise identification of faults. Consequently, each operation must evaluate all potential new entries to identify the requisite shared parity bit or bits. Although the majority of FPGA issues are identified during maintenance, it remains essential to examine the entire configuration frame for potential problems. The proposed method for error detection necessitates numerous parity calculations. Errors can be identified by the utilization of fundamental parity concerns. A discrepancy between the calculated and produced parities will lead to an error. Prompt feedback is transmitted to the error-correction segment, and any newly identified lines are promptly stored in memory.

5. RESULTS AND DISCUSSION

Simulated result of existing TCAM

The objective is to develop a TCAM that is impervious to errors caused by bit-wise manipulation. Constructing an error detection apparatus is the initial and paramount stage. Errors can be rectified by a specific methodology. TCAM can be utilized for data retrieval during error correction. Consequently, SRAMs must be capable of recognizing potential search operations. In this instance, ER-TCAM (Error-Resistant TCAM) is the optimal choice. Upon identification of the Error Correction Vector (ECV) and its transmission to the SRAM's write port, the search operations and error correction processes of the ER-TCAM are conducted concurrently. Currently, this approach is capable of detecting and rectifying just single-bit errors; it is ineffective in the presence of many faults.

ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

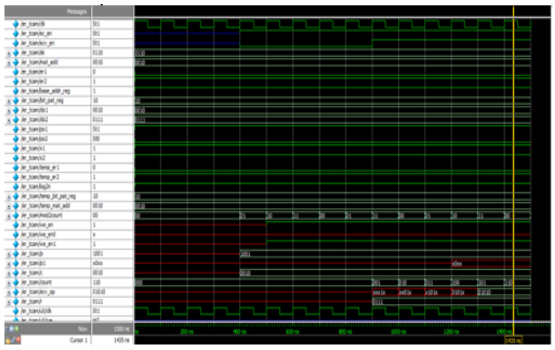

Fig.8 The results of a contemporary Ternary Content Addressable Memory (TCAM) simulation are reported.

Simulated result of proposed ER-TCAM

We developed a distinctive TCAM to facilitate the identification and rectification of errors including three bits or more. This innovative error detection approach employs three parity calculation techniques: diagonal parity, row parity, and column parity. Upon detecting a fault, the machine initiates the restoration operation. The implementation of gate and error locator operations optimizes error correction. Multi-bit defects may be detectable and correctable with the proposed approaches.

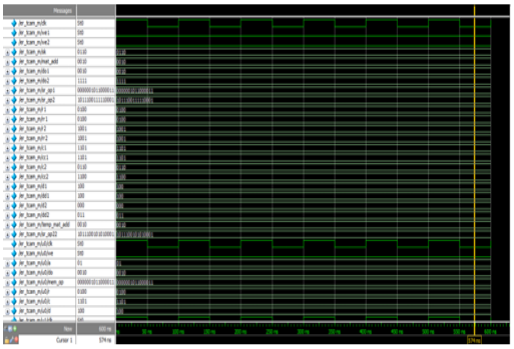

Fig.9 The suggested ER-TCAM's projected outcome is shown.

6. CONCLUSION

Errors in SRAM-based TCAMs can be detected and rectified utilizing the enhanced original data saved on the device. To enhance the circuit and reduce critical route latency, the current error detection method employs a one-bit parity solution. This solution resolves the issues associated with SRAM-based TCAMs by utilizing ER-TCAM, or binary-encoded TCAM tables. The data route is unaffected by the method due to the background error correction utilized by TCAM-enabled SRAMs. The proposed method employs three parities to identify and rectify multibit defects in SRAM-based TCAMs. Addressing small issues is crucial for maintaining the optimal functionality of search engines.

REFERENCES

[1] P. He, W. Zhang, H. Guan, K. Salamatian, and G. Xie, Partial order theory for fast TCAM updates, IEEE/ACM Trans. Netw., vol. 26, no. 1, pp. 217–230, Feb. 2018.

[2] W. Fu, T. Li, and Z. Sun, FAS: Using FPGA to accelerate and secure SDN software switches, Secur. Commun. Netw., vol. 2018, Jan. 2018, Art. no. 5650205.

[3] S. T. Li, H. Liu, and H. Yang, Design and characterization of SEU hardened circuits for SRAM-based FPGA, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 6, pp. 1276–1283, Feb. 2019.

[4] T. Li, H. Yang, H. Zhao, N. Wang, Y. Wei, and Y. Jia, Investigation into SEU effects and hardening strategies in SRAM based FPGA, in Proc. 17th Eur. Conf. Radiat. Effects Compon. Syst. (RADECS), 2019, pp. 1–5.

[5] A. Ramos, R. G. Toral, P. Reviriego, and J. A. Maestro, An ALU protection methodology for soft processors on SRAM based FPGAs, IEEE Trans. Comput., vol. 68, no. 9, pp. 1404–1410, Mar. 2019.

[6] K. K. Gajula, “Reinforcement

ISSN: **3139-5503** | Volume-1 Issue-2 | May-June 2026 | **ADSJ-1203**
DOI: https://doi.org/10.5281/zenodo.22300950

Learning with Transparent Policies: An Explainable AI Approach to Adaptive Cyber Security," American Journal of AI Cyber Computing Management, vol. 5, no. 4, pp. 322–328, 2025.

[7] S. Pontarelli, P. Reviriego, and J. A. Maestro, Parallel D-pipeline: A cuckoo hashing implementation for increased throughput, IEEE Trans. Comput., vol. 65, no. 1, pp. 326–331, Mar. 2015.

[8] P. Reviriego, A. Ullah, and S. Pontarelli, PR-TCAM: Efficient TCAM emulation on Xilinx FPGAs using partial reconfiguration, IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 8, pp. 1952– 1956, Mar. 2019.

[9] K. K. Gajula, "A Hybrid Interpretable AI Framework for Detecting Financial Fraud in Dynamic Transaction Networks," International Journal of Communication Networks and Information Security, 2022.

[10] K. K. Gajula, "Advancing Post-Quantum Cryptography: Novel Algorithmic Models and Security Implementations," Goya Journal, vol. 18, no. 12, pp. 594–605, 2025.

CC BY NC