IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 11, 2022, accepted March 23, 2022, date of publication March 28, 2022, date of current version April 6, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3162890

Security and Privacy of Blockchain-Based Single-Bit Cache Memory Architecture for IoT Systems

REEYA AGRAWAL[1], NEETU FAUJDAR[1], PRADEEP KUMAR[2], AND ANJAN KUMAR[3]
[1]Department of Computer Engineering and Applications, GLA University, Mathura 281406, UttarPradesh, India
[2]Discipline of Electrical, Electronic and Computer Engineering, University of KwaZulu-Natal, Durban 4041, South Africa
[3]Department of VLSI Center of Excellence, GLA University, Mathura 281406, UttarPradesh, India

Corresponding authors: Reeya Agrawal (agrawalreeya0304@gmail.com) and Neetu Faujdar (neetu.faujdar@gmail.com)

ABSTRACT This paper provides an overview of blockchain technology's security and privacy features, as well as an overview of IoT-based cache memory and single-bit six transistor static random-access memory cell sense amplifier architecture. Each chip's memory is used for recorded as blocks, which are encrypted and used as a blockchain for other memory devices. The architectures comprise of the circuit of write driver, six transistor static random access memory cells, and sense amplifiers such as current differential sense amplifier, charge transfer differential sense amplifier, and voltage latch sense amplifier. Furthermore, different parameters such as the number of transistors, sensing delay, and power consumption have been analyzed for varying resistance values (i.e., R=42.3Ω and R=42.3KΩ). Apart from that, power reduction techniques such as dual sleep, forced stack, sleep transistor, and sleep stack are used to optimize power consumption. These power reduction techniques are applied over different blocks of architecture, such as six transistors static random access memory cell and sense amplifier to optimize power consumption of the architecture. The conclusion arises that a single-bit six transistor static random access memory cell with power reduction dual sleep technique voltage latch sense amplifier with power reduction dual sleep technique in architecture consumes 11.65μW of power and has 33 transistors which are lowest from other architectures.

INDEX TERMS Circuit of write driver (CWD), sense amplifier (SA), current differential sense amplifier (CDSA), charge transfer differential sense amplifier (CTDSA), voltage latch sense amplifier (VLSA), six transistor static random-access memory (6T-SRAM).

I. INTRODUCTION

Modern integrated circuits (ICs) carry sensitive data which must be kept safe for concealment. In the last five years, a broad spectrum of attacks on ICs and memories, most of which focused on cache and memory vulnerabilities, smart cards, and other similar devices [1]. The problem worsens when credit cards and other legal papers containing biometrics are targeted because sensitive information is stored in memory. Computer systems receive a lot of attention during execution. Since the recorded data is available quickly after the device loses power, specific primary memory attacks were investigated. These attacks, known as cold-boot attacks, are intended to obtain the latest information stored in the memory [2]. Because the main memory is more accessible in memory systems than other levels of memory, the security is weaker. It can thus be destroyed using less complicated technological means by an attacker. During cold-boot attacks, the information is frozen for a long to remove the memory module and download the material to a backup system that stores data in plain text [3]. To bypass this, during the memory transaction, data is encrypted, which enhances security. An increase in the cache size can make up for the loss of bus performance. Cache memory is now located on the same central processing unit (CPU), either stacked on top of it or incorporated, for performance reasons, unlike main memory [4]. This keeps the data in plain text and keeps the cache-to-CPU performance costs low. In addition, to reduce the need for central memory transfers, several encryption techniques will be implemented in cache memory [5].

A small memory cache is used between the central processor and the main memory unit. A store is physically and

The associate editor coordinating the review of this manuscript and approving it for publication was Hang Shen.

logically closer to the main memory. The top address bits are stored in the tag, while the bottom address bits are stored in the index [6]. Before being used, the cache's contents are purged. The cache memory is divided into several sections. When a specific amount of information is discovered, the central processor unit checks a cache memory to see if it is there; if it is, it is called a cache hit; if it is not, it is called a cache miss [7]. Hit latency and missing latency terms describe delays in such situations. Caches are divided into two types: data storage and instruction storage. Cache memory has several advantages, including high speed, low latency, faster information gathering, and fast data access. Power consumption and area are also essential considerations [8].

A. SECURITY ISSUES IN CACHE MEMORY

A new storage channel testing cache debug capability is used in embedded devices. Interlock, threshold, and ordering algorithms are used in the storage channels. To depict numbers and characters on or off, the author uses the state of variables. The covered canal and the side canal serve as crossing highways. The software characteristics utilized to develop cryptosystems for data transport are called microarchitecture. Famous privilege bits data cache per line is now available via a new covert channel. Covert channels do not use heuristic timings; it was disclosed [9]. The processing of internal and external interruptions in the cache memory of a group of words is part of the encoded mapping of a cache on a cubic basis. The cubic configuration approach remains the corresponding mapping method. Hash features may be an excellent choice. The temporal and geographical position of reference is explored. The objective is to examine the evolution of creative, associative mapping throughout time [10]. Physical memory is known as associative memory. Tag, block, and word are included in the attributes. Cubic cache mapping requires the linear restoration of actual references using a standard approach. Graceful Code (GC) is a probable case study in this respect. The necessity for a state-of-the-art memory test technique is urgently needed. A resource mapping extension is a one-to-one extension. These approaches offer options to improve the cache's design and guard against attacks [11].

Create a cache-like architecture using instructions. Side-channel cache and data assaults cache is utilized for software operations to extract encrypted keys, and hence there is a lack of adequate security [12]. The author uses random permutation software for preloading information. There is a compromise between hardware complexity and overhead performance. A target branch buffer and an updated policy prevent data diffusion. In modular exponentiation, the square matrix multiplying approach is used. Other conditional branches, such as branch target buffer (BTB), should be avoided. For cache attacks, secret keys are necessary. When software and hardware are integrated, data cache protection methods are formed. All the critical data by the exception handler is directed into the cache [13]. Cache-based associative mapping is utilized when the cache memory is designed using a cache controller. The spatial location of the reference point is used. The cache miss ratio is checked by the technique [14]. They can be utilized in processors based on field-programmable gate arrays (FPGA). The cache controller that adjusts the address range in the cache tag memory supplies the microprocessor address range.

When side-channel assaults are common, the safety of a secure cache architecture is challenged. The caching approach uses dynamic memory for eviction-based re-mapping. By slightly altering the substitution method, better results can be produced. Memory exploitation of addresses can find secret keys [15]. Different types of attacks must be considered. Prime and sample attacks can fill the entire cache region with nasty stuff. The spy technique, which includes counting cache hits, is compelling in this scenario. The evict and time attacks are used to determine how long it takes for data to be encrypted. It is possible to improve the replacement algorithm [16]. The new cache does not prevent eviction and time assaults. The new store may work. Mobile devices which use user security and privacy cache memory are subject to time-driven cache attacks. This type has two phases: research and aggression [17]. The correlation step includes an extensive critical search phase.

Energy efficiency in multi-tasking systems is a significant concern in the cache colour technique to reduce leakage energy [18]. Dynamic profiling with dynamic cache reconfiguration is available for the optimum energy efficiency memory subsystem. Improving the efficiency of memory encryption in multi-processor systems considers the most trusted physically attacked chip. Security measures such as confidentiality and integrity are essential beyond the chip [19]. A suitable counter cache technique can be implemented using the consistency protocol. During cache cooperation, the coherence protocol improves the rate of counter cache hits saved. As previously mentioned, these techniques enhance cache memory architecture's overall performance. When side-channel data are detected, the theoretical usage of cache memory on a side-channel based on cryptography is a possible option [20]. Simple text encryption allows for data hacking. Computational power approaches based on techniques like fundamental and differential power analysis can be used to hide confidential data in memory devices. Cache hits, cache misses, and cache size are all significant factors. A store must be shut off to prevent data theft if the power is turned off. A stock is built into a processor to avoid an attack on the algorithm's implementation. Timing skews and spurious operations are included in the approach to confound the intruder [21].

The timing phenomenon is utilized to guard against attack in the software strategy. There is the ability to recover secret keys using particular side-channel attacks. Modifications in algorithms only increase safety to a limited amount. This approach produces encryption that is based on a sandbox [22]. Redundancy instructions are entered as binary codes in a cypher mode. Two components of the sandbox method are the interpreter and the translator. Creation of the

pseudo-random number by reading time stamped counter. Additional time is given through redundancy. Soft errors create transitory failures; thus, lowering costs to protect large caches against errors is a brilliant idea [23]. The last stage is to employ power scaling methods to reduce power. Stores use chip memory designs in today's microprocessors. For this aim, a reorder buffer technique is utilized. In the architecture, several schemes are used. The first approach for repairing and protecting errors is based on dirty cache lines. Cache lines are cleaned, and parity checks are carried out for protection [24].

Attacks come with new cache designs that are easy to run on several platforms. This method does not need the use of any special equipment. In addition, no more computing power is required. The secret key may be retrieved by simply measuring the time. Two essential mitigation techniques are found in this investigation. The primary priority is partition-based work to eliminate interference with the cache memory. The second technique guarantees random cache interference. The technologies presented here provide hardware solutions based on mathematical rules theoretically [25]. Physical security measures are vulnerable to side-channel attacks. Microarchitecture side-channel attacks are being investigated. A memory cache with low power consumption is created. Cache memory with BTB-based branch prediction [26] is a one-of-a-kind type of cache memory. Defensive techniques based on the square and multiplying approaches provide significant results on an algorithmic and architectural level. Conventional attacks attempt to break data by flushing the S-box components from the cache. During the encryption process, a cache miss is introduced, and power traces are used. It is not necessary to empty the cache before encrypting the data. After that, they are added to the cypher's block. There is no need for randomization. Before the actual calculation begins, counter measures are taken by inserting a series of s-boxes into the encryption method [27].

Data screening-based secure data authentication in memories, power reduction and cell stability based on dynamically isolated read static random success storage, and data screening-based secure memory storage data authentication are all thoroughly addressed, with viable solutions. Cache consistency management performance analysis in a mobile environment using agent technology [28] is a possible method for providing cache safety.

B. HOW COULD BLOCKCHAIN TECHNOLOGY BENEFIT FROM THE INTERNET OF THINGS?

Blockchain technology is hype high, then a rough of deception, but might rise again. Enter blockchain, a digital leader technology that enables organizations to engage and record these transactions safely and unchangingly on many computers connected through an interface between peer and peer networks. Recent advances such as the emergence of COVID-19 have led to the blockchain, which has accelerated digital trends with reduced workforce social distance [29].

C. HOW DOES BLOCKCHAIN TECHNOLOGY WORK?

Decentralization means that data storage machines could belong to different entities. In other words, there is a risk that uses sensitive information will be stored and exposed to third parties by default if not appropriately done. Figure 1 shows blockchain for the Internet of Thing applications [30].

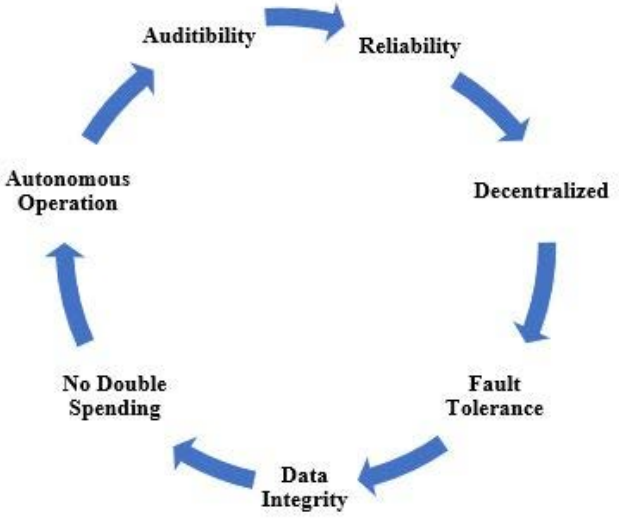

FIGURE 1. Blockchain for the internet of thing applications.

Then users have an immutable data structure that may indicate who and when their data has been viewed. One further step, blockchain technology, can store data access permissions for users. Every third party wishing to have user data must first ask for it, and a request and reply can be kept on the blockchain. Users and requesters now have an immutable database that identifies who has long-term access to precise information [31]. This program can improve the privacy of a data market and provide users with the backbone to benefit from the sale of their knowledge.

D. INTERNET OF THINGS AND BLOCKCHAIN BENEFITS

A distributed blockchain manipulator reduces stakeholder's requirement for confidence between themselves, a senior vice president, and the worldwide payment manager of an information technology (IT) services company. Therefore, no single body controls the large number of data that internet of thing (IoT) devices creates. It is almost difficult for anyone to change current data records with blockchain encryption. And using blockchain to store IoT data gives another security layer to prevent malicious attackers from accessing the network [32]. A critical concern for IoT providers is protecting information throughout the entire IoT ecosystem. IoT devices can easily be a goal of distributed denial-of-service attacks, malicious attackers, and security data breaches. The marriage of IoT and blockchain opens the doors to new opportunities which eliminate inherent inefficiencies, increase security and enhance transparency among all parties involved while allowing safe machine-to-machine transactions [33].

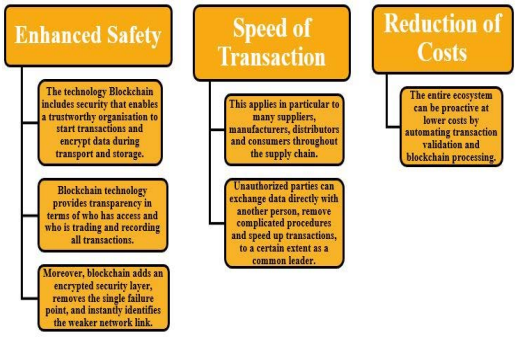

FIGURE 2. Blockchain and IoT are the following advantages.

Figure 2 shows blockchain and IoT advantages. Blockchain is an example that seems like a technology of transformation, but the meaningful implementation of cryptocurrencies above and above has not been achieved [34]. IoT deployments face various challenges, including cost, security, privacy, and data exchange. Although these are different challenges, there are many connections. IoT clients, typically paired by business partners, demand quick and cost-effective IoT data and insights and must be confident. The blockchain may all be the backbone. Blockchain is encrypted and safeguarded with many independent nodes, reviewing chain updates to prevent unpleasant behaviors before upgrades. All parties involved may monitor and confirm the blockchain to increase data availability and confidence without burdensome and costly bureaucratic layers [35].

E. SOLVE THE SECURITY PROBLEM IN CACHE MEMORY USING BLOCKCHAIN TECHNOLOGY

Proponents of blockchain-known distributed ledger technology regard, it as one of the finest solutions to safeguard transactions [36].

1) SECURITY BY THE BLOCKS

Blockchain is a digital block sequence containing transaction data. Each brick is connected to the blocks before and after it. A hacker would have to modify the block holding that record and its links, making it impossible to manipulate a single form to evade discovery [37]. This may not seem to be a dissuasive measure, but blockchain has some fundamental features that give more safety. Cryptography is employed to safeguard blockchain records. The value of early warning to avert future damage cannot be overestimated. Unfortunately, blockchains are decentralized for those determined hackers and extend over regularly updated and synchronized peer-to-peer networks. Blockchains have no single failure point and cannot be changed by a single machine as they are not centrally stored [38].

2) ALL BLOCKCHAINS ARE NOT CREATED EQUAL

Today, there are two main kinds of blockchain: private and public, each with unique characteristics [39]. There are several vital variations between public and private blockchains that might change their level of security. The apparent difference is that public blockchains verify transactions and bundle them in blocks to add machines linked to the repository. Any Internet-connected computer is welcome to participate in the celebration [40]. On the other hand, private blockchains generally enable only known companies to join. When they operate together, they establish a covert, members-only business network. This difference has significant implications for the storage and access of (potentially sensitive) data through the web. Another significant contrast is that public blockchains typically rely on the idea of anonymity.

In contrast, private blockchains rely on identification to validate their membership and access credentials that enable network participants to know who they interact with specifically. For a blockchain to be included, network participants must agree that the transaction is the sole version of the truth [41]. On the other hand, a private blockchain is an authorized network in which a method called ''selected endorsement'' reaches consensus, in which recognized users validate transactions.

3) A BLOCKCHAIN NETWORK IS ONLY AS SECURE AS IT's INFRASTRUCTURE

Blockchain has inherent safety features, recognized infrastructure vulnerabilities can be exploited by unscrupulous actors. Prevent anybody, even root users and managers, from accessing sensitive data. Encryption keys should be maintained appropriately to guarantee that they are never misused utilizing the highest security standards. Blockchain platform to discover more about the first fully integrated blockchain platform for companies designed to speed up the building, governance, and managing of a multi-agency network [42].

F. INTERNET OF THINGS MEMORY: AN OVERVIEW

Internet of things develops at a dizzying pace; designers have created new difficulties and opportunities. On the other hand, do not forget about the gadget's memory requirements. The rapid rise of the Internet of Things has presented new opportunities and difficulties for designers [43]. Any new IoT technology or update to an older one will have memory needs that must be met. The number of memory options for IoT devices has not yet reached the market, but choosing what to add may feel like that.

1) MEMORY CONSIDERATIONS

The device priorities are the first item to consider while considering memory options. Depending on the device, the author may need to consider the following factors [44], as shown in Figure 3.

2) INTERNET OF THINGS (IoT) MEMORY TYPES

Embedded technology developers usually use one of the following options to choose memory. Figure 4. shows IoT Memory Types [45].

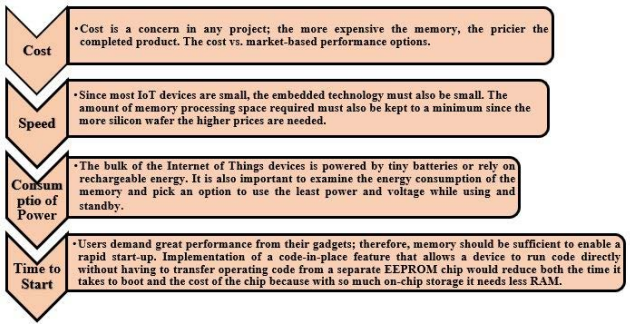

FIGURE 3. Factors of memory consideration.

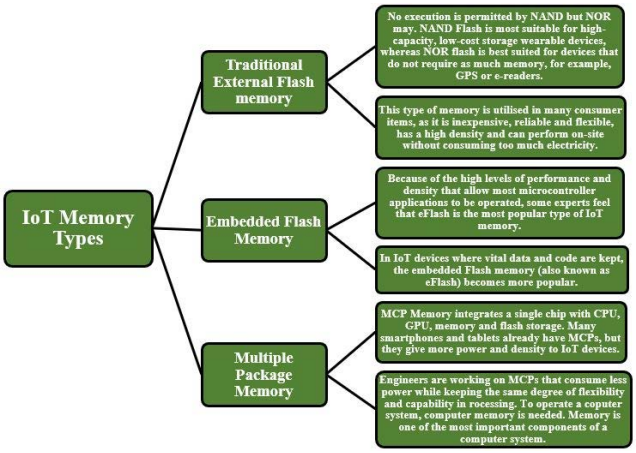

FIGURE 4. IoT memory types.

3) WHAT IS MEMORY OF COMPUTERS?

Memory of computer is important because a computer cannot do anything unless it has enough memory to do it.

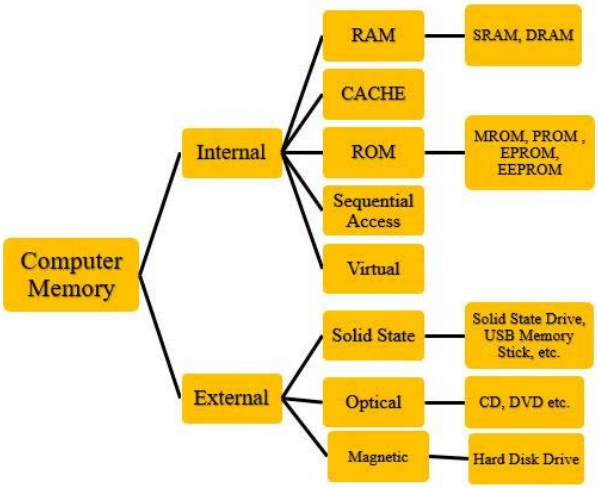

FIGURE 5. Computer memory classification.

The memory [46] is where data and instructions for performing specific computer system tasks are kept. Data can be stored and retrieved from the computer's memory. Building blocks of memory are the individual memory cells that make up memory. The unique address of a memory cell refers to the index or identifier number assigned to each memory cell in a computer system. The central processing unit (CPU) is in charge of figuring out which memory cells need data sent to them or read from them. The system's performance is influenced by the computer's random access memory (RAM) and CPU [47]. The CPU has a limited capacity for storing vast amounts of data or applications. The classification of computer memory is shown in Figure 5 [48].

4) A BLOCKCHAIN NETWORK IS ONLY AS SECURE AS ITS INFRASTRUCTURE

Embedded multimedia cards (eMMC) provide large amounts of storage for a low price while also providing outstanding performance and requiring little power when in use, making internet of things devices more affordable. [49]. The cards feature bespoke controllers that make interfacing with application systems easier. The fact is that eMMC is among the finest owing to its capacity to handle many operations simultaneously and therefore increase its speed by up to 30%. The cards also provide better security by extending the basic type-protection capabilities to prohibit rewriting or deleting user data without authorization [50].

Section I describes the introduction of IoT, the relationship between IoT and blockchain, how blockchain works, what is computer memory, IoT memory types, solving the security problem in cache memory using blockchain technology and IoT, and blockchain benefits. Subsections of I describe the following security issues in the cache memory, how blockchain technology benefits the IoT, and the solution of a security problem using blockchain technology. IoT memory: An overview moving toward the II section is a review of recent papers on IoT, blockchain, and cache memory. Section III is divided into four subsections and discusses power reduction techniques. A subsection of section III describes the power reduction dual sleep technique, the power reduction sleep transistor technique, the power reduction sleep stack technique, and the power reduction forced stack technique. Section IV describes the single-bit 6T-SRAM SA architecture's functional block diagram, divided into three subsections, and describes CWD working and schematic, 6T-SRAM Cell working and schematic, and different sense amplifiers like CDSA, CTDSA, and VLSA. Section V describes simulated result analysis and discussion. The conclusion of the paper is described in Section VI. The shortcomings of single-bit 6T-SRAM SA architecture are consumption of power and delay in sensing. To optimize consumption of power, techniques of power reduction are applied and due to this reason number of transistors are increases and the area increases.

II. LITERATURE REVIEW

Blockchain, the internet of things, and artificial intelligence (AI) breakthroughs are no longer a secret because of their potential to change company structures and disrupt entire

industries. Blockchain, for example, provides a shared and decentralized distributed ledger that improves trust, transparency, security, and privacy in corporate processes. These details almost all relate to money or identification. Because of the internet of things (IoT) in, German and European enterprises must focus on automation and user-friendliness [51].

The cloud simplifies data storage, processing, and transfer. Despite the current cloud-centered design, which enables rapid deployment of IoT applications, isolated data silos have hampered the potential of IoT for holistic data analysis. Instead of accessing data by a centralized privacy authority, the authors provide people autonomy over their data. Data streams from IoT devices necessitate a specialized framework. The author uses blockchain as an auditable and distributed control layer for secure and dependable storage layer access. This decentralized storage system uses blockchain technology to keep track of time-series data generated by IoT devices [52].

Intelligent health systems are already capable of providing increasingly sophisticated services in real-time, due to this rapid expansion of the internet of medical things (IoMT). When it comes to privacy and security, the Internet of Things creates serious issues. Because of the extensive range of devices, it is also impossible to develop a single security standard solution. Instead of a decentralized IoMT healthcare system, current IoMT healthcare systems rely on cloud computing for electronic health record (EHR) and medical services, which is unsustainable. While retaining system security and privacy for all parties involved, the authors suggest a new Blockchain-based architecture for decentralized EHR and intelligent contract-based service automation. Researchers have combined a distributed blockchain data storage system with a hybrid computing paradigm in our architecture to address some of the shortcomings of blockchain-based cloud-centric IoMT health systems, such as excessive latency, high storage costs, and a single point of failure. Researchers created a selective ring-based access monitoring system with device authentication and patient anonymity algorithms to make the system more secure. This system is decentralized and selective. The author has studied the proposed system's data interchange latency and cost-effectiveness. According to the author's logical analysis, our architecture-based security and privacy solutions meet the decentralized IoMT innovative health systems [2].

Blockchain and IoT are the mottoes in the information technology (IT) community. Both advancements have a significant influence on our everyday lives. The internet collects and supplies enormous amounts of information from worldwide. IoT contains heterogeneous devices interacting across numerous networks, conveying sensitive and uncritical data, creating safety and administration concerns for data collection. For IoT-based data transfer, a secure blockchain-based architecture is proposed [53].

The internet publishes and exchanges enormous amounts of data every day. Small data components enable machine-to-machine communication as the IoT grows and add network edge reading sensors and actuators. IPv6 datagram messages are commonly utilized as IoT content objects. End-to-end Internet protocol transmission and security are frequently used in IoT connections [54].

IoT is rapidly gaining popularity. Our homes and hospitals are full of sensors that monitor environmental changes and provide various beneficial services. The increased use of IoT raises several security concerns. IoT architecture is described first, followed by the safety issues, technical challenges, and requirements found inside the three-layer structure. There are investigations into the following topics: threats to the IoT and countermeasures and preventative measures to be implemented in each domain [55].

The core IoT infrastructure comprises applications, gateways, processors, and sensors. Low-power and high-speed memory, such as six transistors static random-access memory (6T-SRAM) and read only memory (ROM), is required for these subsystems. High-speed or low-power applications can determine how much memory is needed for IoT applications. Mobile and handheld devices require ultra-low power 6T-SRAM as low-power gadgets become more common. At the same time, the 6T-SRAM's performance should not be harmed. Wearable devices are the newest trend, and 6T-SRAMs with ultra-low power consumption are required. The application determines the amount of memory needed in IoT systems. Dynamic random-access memory (DRAM) and flash memory, for example, are used in applications that require a large amount of data storage and management. Fast 6T-SRAM memory is necessary for applications requiring a high transmission rate [56].

Due to its excellent performance, 6T-SRAM cache memories are frequently utilized. The 6T-SRAM chip is a crucial component of system on chips (SOCs) because they regulate energy consumption and operational speed. The low power 6T-SRAM is therefore vital. Low power design has been a significant problem in current portable and small chip designs as complementary metal oxide semiconductor (CMOS) has declined. Speed, power consumption, size, and dependability to enhance performance are the critical areas of concern in today's technology [57].

To bridge the programming execution over numerous power cycles, intermittent IoT devices typically leverage emerging non-memory technologies. Cache contents are cross-checked with non-volatile memory register contents during power outages. Despite being a pure non-volatile cache, it has low efficiency due to its high write latency and energy costs. A quick restart is possible using this technique even when there isn't a considerable cache condition [58].

Gupta, Navneet, *et al.* [2021] These memories use classic differential sensing to store data. Because of the unidirectionality of TFETs, which makes it impossible to give a SA differential output, single-end sensing is a possible alternative to enhanced tunnel field-effect transistor (TFET) memory cells. As a result, single-end sensing is employed in most recent TFET memories for reading. The bulk of TFET memory bit cells mentioned in the literature uses static power

several decades below their CMOS equivalents. However, their performance is limited. As a result, the major challenge with creating single-end sensing is to rely upon the use of a tiny sense amplifier (SA) to differentiate the 1 and 0 while minimizing a necessary bit line voltage loss [59].

SA plays a vital role in memory circuit design, operation, and durability. The proposed circuit is a PMOS SA with high output impedance, minimal sense delays, and low power use. The proposed course performs the same duties as the existing circuits but reduces sensing delay and less power usage [60].

The architecture of semiconductor memory devices is a fascinating subject in and of itself. The cell's structure and topology are mapped out using cutting-edge technologies. As a result of the suggested memory architecture's attention to low-power designs and, more critically, system requirements increase memory performance while also taking the type of memory unit desired for specific technology and application into account. Memory architecture and peripheral components are the study's primary concerns. Designing memory begins with specifying the architecture and organization of individual memory cells [61].

A technological decline leads to a decrease in voltage supply, leading to power leakage. The data stability of 6T-SRAM cells is dependent on the most prominent direct current (DC) noise, which can be ignored on the intercoupled outputs of the inverters without damaging the data. The finger approach is used to design different 6T-SRAM cells that reduce the cell's surface area. This technique also required the removal of the parasite in the layout design. After the simulation, it was found that the performance of the 10T design exceeds all other 6T-SRAM simulated cells [62].

As technology improves, so does the capability required by the latest technological devices. Electrical appliances depend on the 6T-SRAM cache to provide this level of security. 6T-SRAM cells have recently been developed to address these issues. However, achieving balanced performance across all sub-nanometer technology's 6T-SRAM cell attributes. The novel 6T-SRAM design proposed aims to boost performance by several folds. The cell uses the stacking strategy to reduce energy usage [63]. There are three types of leakage reduction solutions for modern 6T-SRAM: latches bit lines and read ports. 6T-SRAM is sensitive to both inter-die and intra-die process changes, the multi-threshold CMOS approach, drowsy mode, and Substrate-biased approaches have the most remarkable ability to reduce latch leakages [64].

III. TECHNIQUES OF POWER REDUCTION

Techniques of power reduction can be utilized in many circuits to reduce power consumption, increasing the number of transistors used in the design [65]. The following are some examples of techniques.

A. POWER REDUCTION DUAL SLEEP TECHNIQUE

Dual sleep technique makes use of two PMOS transistors and two NMOS transistors. Both PMOS and NMOS are utilized in the header and footer. In the inactive mode, one transistor is turned on while the other is switched to the off state of operation. Figure 6 shows how PMOS and NMOS store energy when a computer is in sleep mode.

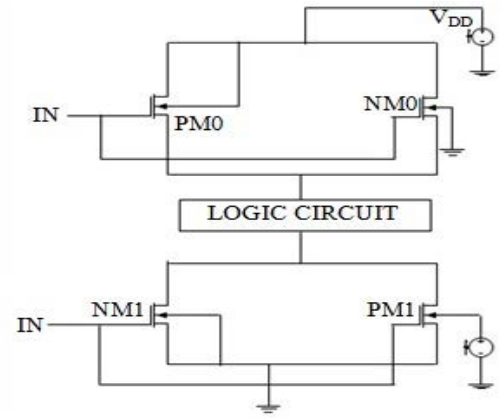

FIGURE 6. Power reduction dual sleep technique.

B. POWER REDUCTION SLEEP TRANSISTOR TECHNIQUE

In this technique between the VDD and the upstream network, there is a high-threshold sleep transistor, and between the downstream network and the GND, there is another sleep transistor. These transistors are activated when the circuit is turned on or off, as indicated in Figures 6 and 7 [66].

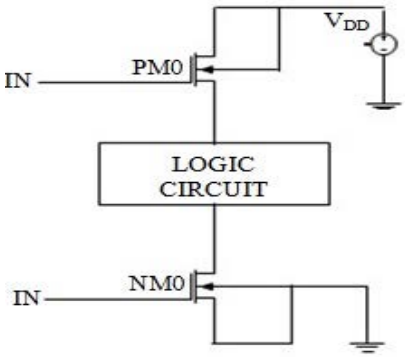

FIGURE 7. Power reduction sleep transistor technique.

C. POWER REDUCTION SLEEP STACK TECHNIQUE

The forced stack is combined with a sleep transistor for maximum efficiency using a sleepy stack. Compared to using a forced stack, the sleeping stack technique uses high transistors with latency penalties and is in sleep mode in the same logical state as the forced stack. As illustrated in Figure 8, this results in sleepy stack technology using ultra-low leakage power while still keeping a superior form [67].

D. POWER REDUCTION FORCED STACK TECHNIQUE

The force stack technique reduces sub-threshold leakage current by doubling the size of an existing transistor.

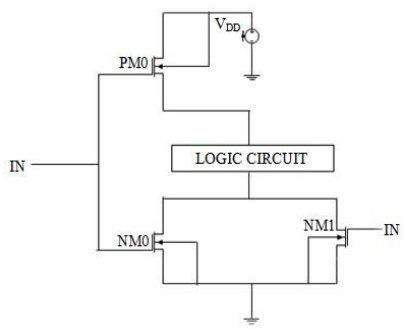

FIGURE 8. Power reduction sleep stack technique schematic.

The transistor's present state can be saved even after it has been turned off. Because of the significant increase in latency (as seen in Figure 9), the high Vth transistor cannot be used in this design [68].

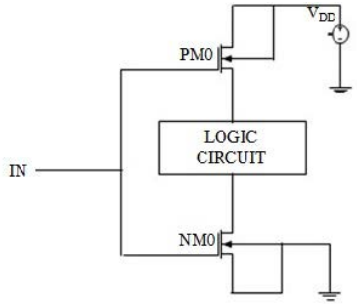

FIGURE 9. Power reduction forced stack technique schematic.

IV. FUNCTIONAL BLOCK DIAGRAM OF SINGLE-BIT 6T-SRAM SA ARCHITECTURE

CWD, 6T-SRAM, and SA are the three blocks that make up the Cache Memory Design Macro (such as CDSA, CTDSA, and VLSA).

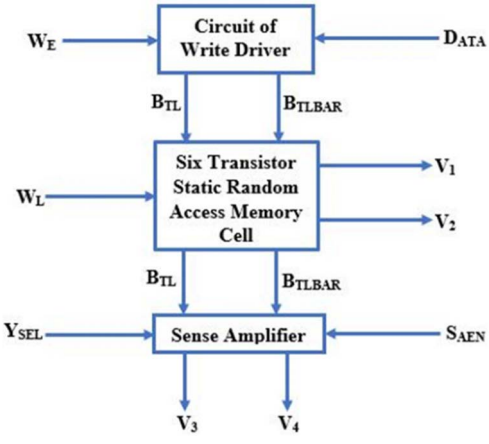

FIGURE 10. Functional block diagram of single-bit 6T-SRAM SA architecture.

The 6T-SRAM macro connection connects these four units. The array of 6T-SRAM is what makes up the memory module. As well as controlling various control signals, the control unit generates and operates a circuit comprising a write driver and a sensing amplifier [69]. Figure 10 depicts the single-bit 6T-SRAM SA architecture's functional block diagram. Cache memory design for single-bit architecture comprises CWD, 6T-SRAM, and CDSA, as shown in Figure 11 [70].

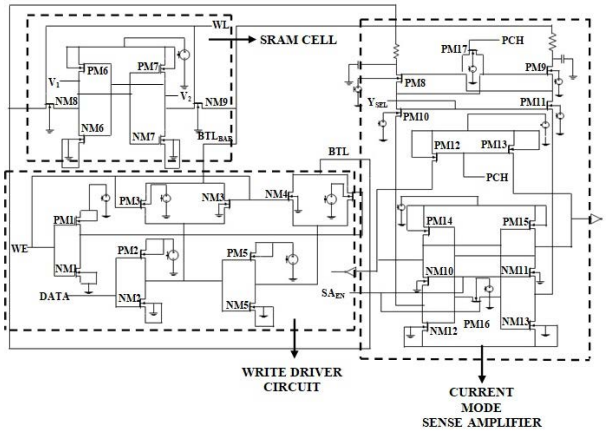

FIGURE 11. Single-bit 6T-SRAM CDSA architecture schematic.

It is separated into three parts:

a) CWD has two i/p pins (Word Enable (W_E) and D_{ATA}) and two o/p pins (B_{TL} and B_{TLBAR}).
b) 6T-SRAM is a connection to the CWD through bit lines and has one i/p pin (Word Line, i.e., W_L) and two o/p pins (V_1 and V_2), and is connected to the sa via bit lines with capacitance and resistance.
c) SA has two o/p pins (V_3 and V_4) whereas four i/p pins (Y_{SEL}, S_{AEN}, B_{TL}, and B_{TLBAR})

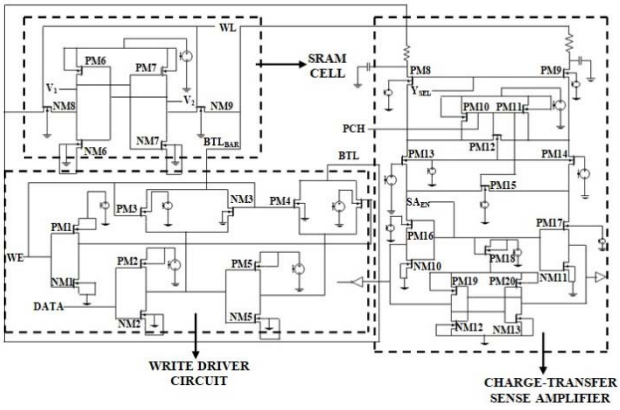

FIGURE 12. Single-bit 6T-SRAM CTDSA architecture schematic.

CWD, 6T-SRAM, CDSA, CTDSA, and VLSA as shown in Figure:11, Figure 12, and Figure 13, respectively [71].

A. CWD WORKING AND SCHEMATIC

The circuit of write driver (CWD) writes the data in the 6T-SRAM. CWD decreases the write margin. The role of the

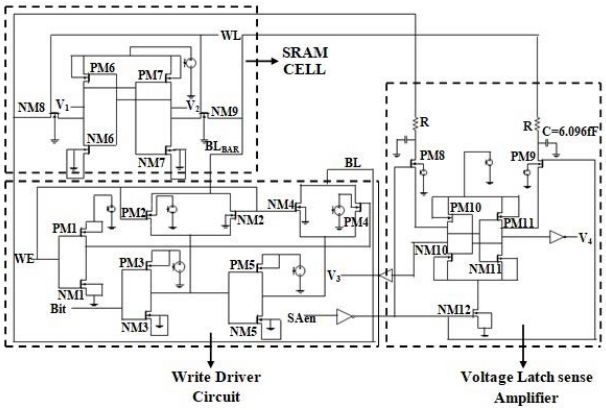

FIGURE 13. Single-bit 6T-SRAM VLSA architecture schematic.

circuit is to charge or unload the bit lines to the desired bit in the memory cell. It is a ten-transistor design having five Pmos (PM1, PM2, PM3, PM4, and PM5) and five Nmos (NM0, NM1, NM2, NM3, NM4, and NM5). It has two input pins, W_E and D_{ATA}, and two output pins, B_{TL} and B_{TLBAR}, connected to the 6T-SRAM access transistors. The data that users desire would be reported to bit lines if they were loaded into CWD. It is seen in Figure 14 that if W_E are H_{IGH}, the D_{ATA} pin value will be stored on the bit lines [72]. Data is written to 6T-SRAM using CWD.

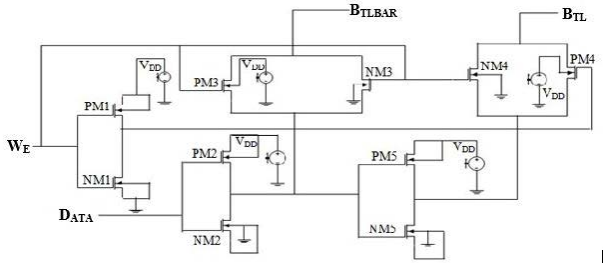

FIGURE 14. CWD schematic.

B. 6T–SRAM CELL WORKING AND SCHEMATIC

6T-SRAM has named six random-access static transistors. It has a property for a long time before the power supply is supplied to store the data [73]. 6T-SRAM cells are made up of two CMOS (CMOS latch) transistors that are back-to-back and each of which is dependent on the data in the other two transistors (i.e., single-bit). Bit lines provide access to the data stored in the 6T-SRAM. It is the most common memory cell because it is the least stable and dissipates the least static electricity. As shown in Figure 15, when W_L Is HIGH, the access transistors can perform read and write operations restricted to the cell's bit lines [74]. This 6T-SRAM comprises two cross-connected CMOS inverters (two pull-up transistors (PM6 AND PM7), two pull-down transistors (NM6 AND NM7), and two access transistors (NM8 AND NM9). Each bit is a 6T-SRAM which holds two-transistor cross-connected inverters. In this storage cell, there are two stable states equivalent to 0 and 1 [75].

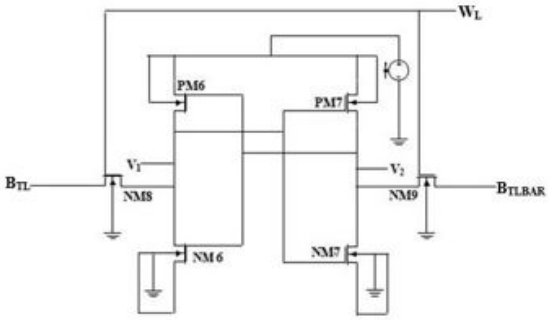

FIGURE 15. 6T- SRAM cell schematic.

C. SENSE AMPLIFIER

The sensing amplifier is a component of the memory cache design. One of the bits is drained by reading, while the other remains at the power supply. The delayed release is caused by the VAST bit lines capacity and the limited access to the bit cell transistors. A slight discrepancy is broadened by the SA between the bit line voltages and the digital levels [76].

1) CDSA WORKING AND SCHEMATIC

As shown in figure, one-bit line, as shown in figure 16, releases while the other is still at a voltage. this is achieved by SA enhancing minor changes in the voltages of the bit line on digital levels [77]. The current sensory differential amplifier is split into two parts:

a) current circuit of transportation with current unit gain transfer characteristics,

b) current differential sensing detects differential current detection amplifier.

The internal nodes $SA_1$and SA_2 are already set up using a Pmos to have the same delay and latching time for each read cycle. The second current sense amplifier, which is used to measure the amount of current, is connected to the output of the current-transport circuit.

2) CTDSA WORKING AND SCHEMATIC

CTDSA is the part that picks up on the difference in the amount of electricity that flows. PMOS transistors with positive feedback are used in this case. there are four PMOS transistors (PM8, PM9, PM10, AND PM11) with positive feedback. Internal nodes SA_1 and SA_2 are already set up to have the same delay and latching time each time they are read. The output of the current-transport circuit is connected to the second current sense amplifier.

The charge will be transferred from the high bit-line capacity to the low-capacity amplifiers SA_5 and SA_6. The swing of the bit line is shallow and the velocity relatively HIGH [78]. The second portion of CTDSA latches the output of common gate amplifier nodes SA_5 and SA_6 and forms a cross-coupled inverter from transistors PM18, PM19, PM20, NM12,

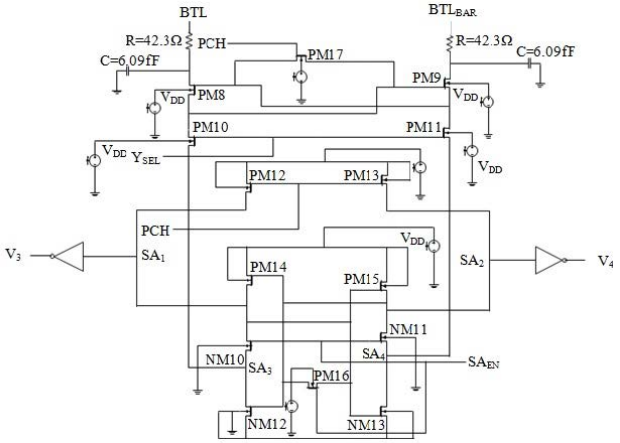

FIGURE 16. CDSA schematic.

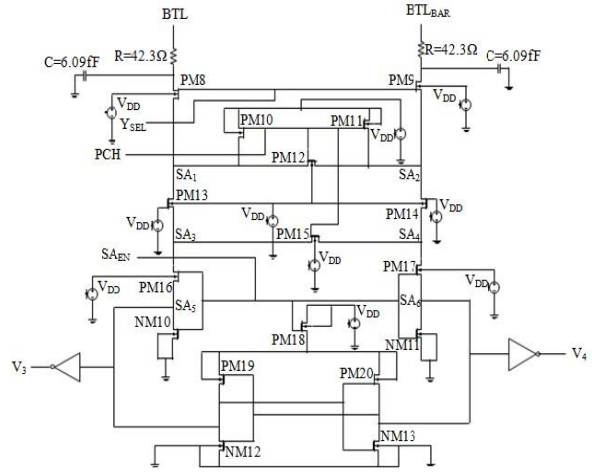

FIGURE 17. CTDSA schematic.

AND NM13. When S_{AEN} falls below a certain threshold, CTDSA is activated. Assume bit-line B_{TLBAR} falls LOW and its voltage moves to Vb + |Vtp|, causing voltage PM13 to enter the sub-threshold zone of operation, stopping the charging of output node SA_6, while the other bit-line stays HIGH and node SA_5 is charged HIGH, as illustrated in figure 17 [79].

3) VLSA WORKING AND SCHEMATIC

Figure 18 depicts the VLSA design, and the differential voltage on the bit lines are resolved to a full swing at the output by the inverters PM10, PM11, NM10, AND NM11. This architecture's internal nodes are pre-charged using the bit-lines [80]. A voltage differential between the input bit lines and the circuit's internal nodes is created by the circuit design directly. When the W_L is HIGH and before the sensing amplifier is triggered, NM12 is off and pass transistors PM8 and PM9 are on. As the differential on the bit lines grows, the internal nodes of the SA have an acceptable voltage difference. The four cross-coupled inverters PM10 and PM11,

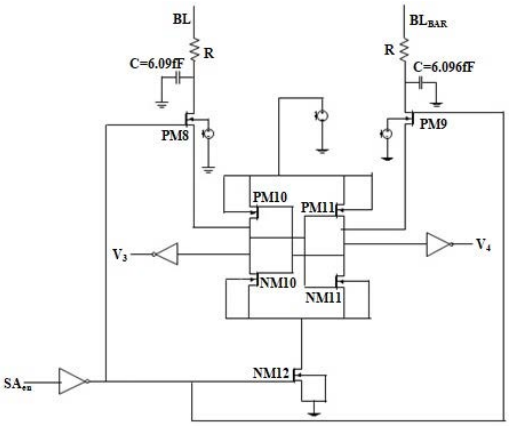

FIGURE 18. VLSA schematic.

as well as the two n-channel NM10 and NM11 amplifiers, boost the sense signal S_{AEN} when it is asserted [81].

V. SIMULATION RESULTS AND DISCUSSION

In this section, all the circuit output waveform has been elaborated. Analysis of different parameters such as the number of transistors and consumption of power of varying architecture has been compared. After applying techniques of power reduction over other blocks in architecture, consumption of power and the number of transistors were analyzed.

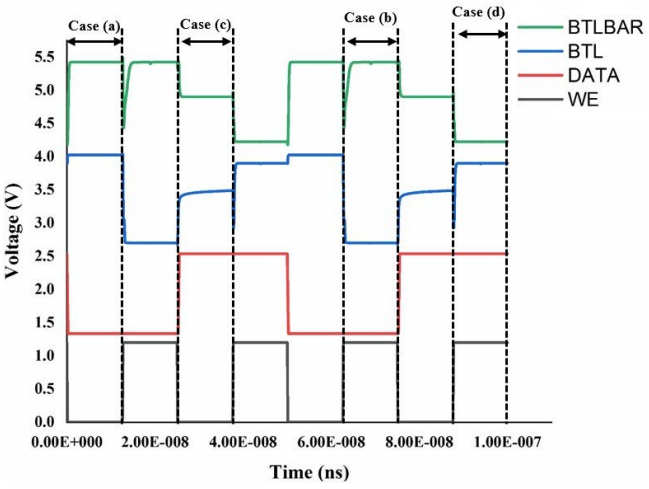

FIGURE 19. CWD waveform.

Figure 19 shows the CWD output waveform. It can be described in four cases:

Case a): W_E are LOW, and D_{ATA} is LOW B_{TL} = HIGH and B_{TLBAR} = HIGH,

Case b): W_E are HIGH and D_{ATA} is LOW B_{TL} = LOW and B_{TLBAR} = HIGH,

Case c): D_{ATA} is High and W_E are LOW, B_{TL} = B_{TLBAR} = HIGH/2

Case d): D_{ATA} IS HIGH, AND W_E ARE HIGH B_{TL} = HIGH AND B_{TLBAR} = LOW.

Figure 20 depicts the 6T-SRAM process in writing and holding. A pull-up network PM6 and PM7 are the transistors of the pull-up network, NM8 and NM9 are access transistors, and NM6 AND NM7 are pull-down network transistors that enable the storage of data and sensing amplification for data reading. There are two basic rules that cells must follow to work well with 6T-SRAM.

- The Nmos (NM6 and NM7) pull-down network transistors must be approximately equal to or more potent than the access transistors (NM8 and NM9). This rule ensures read operation stability.
- The Pmos (PM6 and PM7) pull-up network transistors should be approximately equal to or less than the access transistor (NM8 and NM9). This rule ensures that the value stored in the bit-cell is exchanged during the write operation.

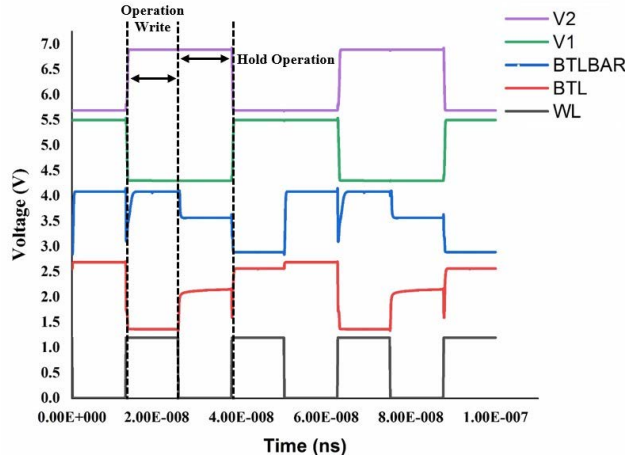

FIGURE 20. 6T-SRAM waveform.

Figure 21 shows the CDSA read process; as both S_{AEN} and W_L are pulled HIGH, only SA senses 6T-SRAM data at bit lines and outputs at V_3 and V_4 during that period

The bit-lines and the output nodes SA1 and SA2 are pre-charged. YSEL is HIGH, PCH is LOW, PM8 and PM9 are in active mode due to, while PM10 and PM11 are in the cut-off mode, which causes data at bit lines in the form of current to be stopped at nodes SA1 and SA2 and charge the bit lines, causing nodes SA3 and SA4 to be pre-discharged to ground as because PM12 and PM13 are in active mode, WL is LOW, i.e., no YSEL is LOW during the evaluation phase, pre-charge circuits remain high to pre-charge the bit lines, and PM8 and PM9 are cut-off.

Figure 22 depicts CTDSA reading operation while the S_{AEN} = HIGH and W_L = HIGH amplifiers are active. While PM10, PM11, AND PM12 are in the cut-off mode, data on the bit-lines is passed from 6TSRAM to SA at nodes SA_1 and SA_2. W_L of 6T-SRAM remains HIGH for reading operation, i.e., access transistors are turned on, and B_{TL} is LOW. B_{TLBAR} is HIGH, indicating that the voltage difference at the output (V_3 and V_4) is HIGH. S_{AEN} is LOW (for half positive cycle of W_L) SA detects the difference between B_{TL} and B_{TLBAR},

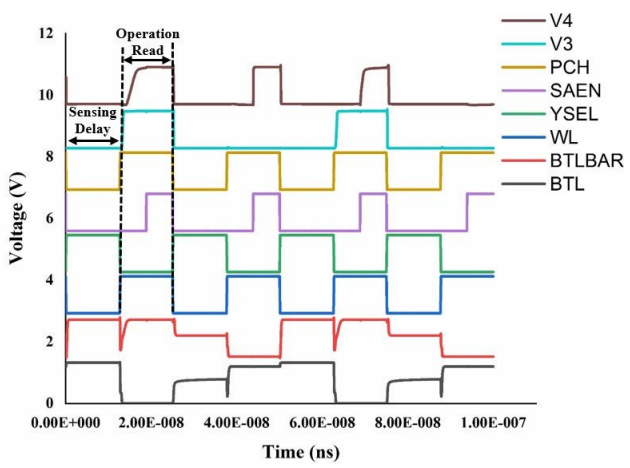

FIGURE 21. CDSA waveform.

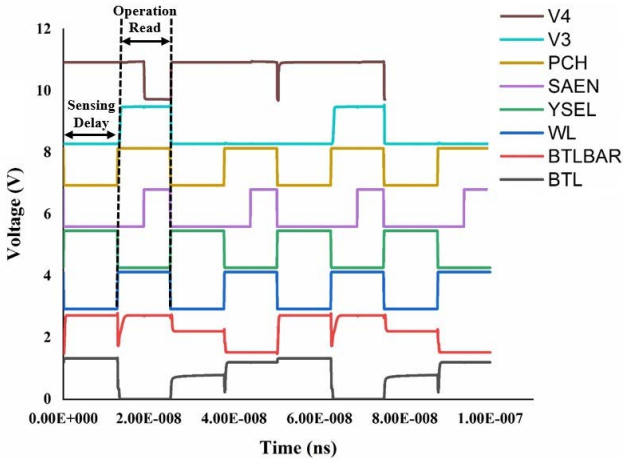

FIGURE 22. CTDSA waveform.

and the stored data is detected because PM16, PM17, AND PM18 are in active mode if B_{TLBAR} is discharging. When B_{TL} is HIGH, the output nodes SA_5 are charged to HIGH, and stored data can be sensed via V_3. Y_{SEL} is LOW, pre-charge circuits are HIGH TO pre-charge the bit-lines, data on the bit-lines is passed from 6T-SRAM to SA, W_L of 6T-SRAM is HIGH for reading operation, and B_{TL} is LOW.

The VLSA reading operation is shown in Figure 23, while the S_{AEN} = HIGH and W_L = HIGH amplifiers are operational during the reading operation. Table 1 compares single-bit 6T-SRAM cdsa architecture, single-bit 6T-SRAM ctdsa architecture, and single-bit 6T-SRAM VLSA architecture parameters at various resistance values. The table shows that the transition between 6T-SRAM and SA in a given architecture does not affect other parameters. Table 1 shows that single-bit 6T-SRAM CDSA architecture consumes 13.96μW of power with 33 transistors, the lowest of all the architectures at R = 42.3KΩ. in Table 1, Table 2, Table 3 and Table 4, CP denotes consumption of power, nt indicates the number of transistors

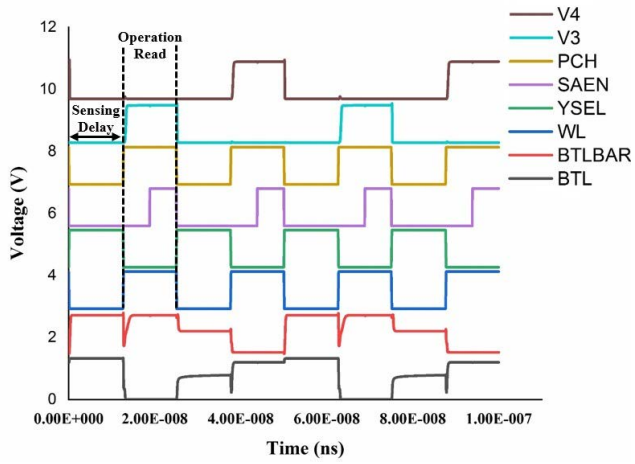

FIGURE 23. VLSA waveform.

TABLE 1. Single-bit 6T-SRAM SA architecture different parameters at VDD = 1.2V, C = 6.09fF.

PARAMETER	SINGLE-BIT 6T-SRAM CDSA ARCHITECTURE		SINGLE-BIT 6T-SRAM CTDSA ARCHITECTURE		SINGLE-BIT 6T-SRAM VLSA ARCHITECTURE	
	CP	NT	CP	NT	CP	NT
R=42.3Ω	14.87μW	33	46.35μW	37	36.57μW	29
R=42.3KΩ	13.96μW	33	44.32μW	37	14.32μW	29

TABLE 2. Single-bit 6T-SRAM SA architecture different parameter analysis on applying TPR over 6T- SRAM in architecture at VDD = 1.2V, C = 6.09fF.

TPR over 6T-SRAM	Single-bit 6T-SRAM CDSA Architecture		Single-bit 6T-SRAM CTDSA Architecture		Single-bit 6T-SRAM VLSA Architecture	
	CP	NT	CP	NT	CP	NT
PRDST	13.05μW	37	41.75μW	41	13.12μW	33
PRSTT	12.84μW	35	41.71μW	39	12.21μW	31
PRSST	14.14μW	36	43.21μW	40	13.36μW	32
PRFST	12.10μW	35	41.71μW	39	12.29μW	31

In Table 2, Table 3 and Table 4, PRDST denotes power reduction dual sleep technique, PRSTT denotes power reduction sleep transistor technique, PRSST denotes power reduction sleep stack technique, prfst denote power reduction forced stack technique.

Table 2 compares the consumption of power and area (in terms of the number of transistors) of single-bit 6T-SRAM SA architecture and concludes that single-bit 6T-SRAM with PRFST CDSA architecture consumes 12.10μW of power with 35 transistors, which is the lowest as compared to other transistors.

Table 3 compares the consumption of power and area (in terms of the number of transistors) of single-bit 6T-SRAM SA architecture and concludes that single-bit 6T-SRAM VLSA with PRFST in architecture consumes 13.57μW of power with 31 transistors, which is the lowest when compared to other architectures.

Table 4 compares the consumption of power and area (in terms of the number of transistors) of single-bit 6T-SRAM SA architecture when TPR is applied to 6T-SRAM and SA (such as CDSA, CTDSA, and VLSA) and describes the different parameters on using TPR to 6T-SRAM and SA (such as CDSA, CTDSA, and VLSA). As a result, single-bit 6T- SRAM with PRDST VLSA with PRDST in architecture consumes 11.62μW of power with 33 transistors, which is the lowest among the others.

TABLE 3. Single-bit 6T-SRAM SA Architecture Different Parameter Analysis on Applying TPR over SA in Architecture at VDD = 1.2V, C = 6.09fF.

TPR applied over SA	Single-bit 6T-SRAM CDSA Architecture		Single-bit 6T-SRAM CTDSA Architecture		Single-bit 6T-SRAM VLSA Architecture	
	CP	NT	CP	NT	CP	NT
PRDST	13.82μW	37	20.38μW	41	13.58μW	33
PRSTT	13.75μW	35	20.38μW	39	13.62μW	31
PRSST	13.90μW	36	19.75μW	40	13.67μW	32
PRFST	13.63μW	35	21.05μW	39	13.57μW	31

TABLE 4. Single-bit 6T-SRAM SA architecture analysis of different parameters on applying TPR over 6T-SRAM and SA in architecture at VDD = 1.2V, C = 6.09fF.

TPR over 6T-SRAM and SA	Single-bit 6T-SRAM CDSA Architecture		Single-bit 6T-SRAM CTDSA Architecture		Single-bit 6T-SRAM VLSA Architecture	
	CP	NT	CP	NT	CP	NT
PRDST	13.05μW	37	18.18μW	41	11.62μW	33
PRSTT	12.52μW	35	18.17μW	39	12.33μW	31
PRSST	14.13μW	36	18.98μW	40	12.69μW	32
PRFST	13.52μW	35	18.19μW	39	11.71μW	31

VI. CONCLUSION

The paper describes the implementation and analysis of a single-bit 6T-SRAM SA architecture made up of 6TSRAM, CWD, AND different types of SA such as CDSA, CTDSA, and VLSA. Apart from IT, all the architecture consumption of power and number of transistors has been analyzed at different values of resistance (such as R = 42.3Ω and R = 42.3KΩ) which acts as a connector between 6T-SRAM cell and sense amplifier. People in today's world want a device that can be easily portable from one location to another, so they require a device that consumes LOW power by market and user requirements. Furthermore, power reduction techniques are used to optimize the consumption of power of architectures, power reduction techniques are applied over different blocks of architectures, such as 6T-SRAM AND SA. The conclusion arises that single-bit 6T-SRAM with PRDST VLSA with PRDST in architecture consumes 11.65μW of power and has 33 transistors which are the lowest among the other architectures. There will always be a tradeoff between power consumption and area. In the future, researchers can use this work in the form of an array.

REFERENCES

[1] B. Nour, K. Sharif, F. Li, and Y. Wang, "Security and privacy challenges in information-centric wireless Internet of Things networks," *IEEE Secur. Privacy*, vol. 18, no. 2, pp. 35–45, Mar. 2020.
[2] B. S. Egala, "Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, Jul. 2021.

[3] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17236–17260, Dec. 2021.

[4] X. Yang, "Blockchain-based secure and lightweight authentication for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3321–3332, Mar. 2022.

[5] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for Internet of Things," *Sensors*, vol. 21, no. 3, p. 772, 2021.

[6] P. Ruf, J. Stodt, and C. Reich, "Security threats of a blockchain-based platform for industry ecosystems in the cloud," in *Proc. 5th World Conf. Smart Trends Syst. Secur. Sustainability (WorldS4)*, Jul. 2021, pp. 192–199.

[7] S. Velliangiri, "Blockchain based privacy preserving framework for emerging 6G wireless communications," *IEEE Trans. Ind. Informat.*, early access, Aug. 27, 2021, doi: 10.1109/TII.2021.3107556.

[8] A. Ahmed and S. Abdullah, "Cloud-based energy efficient and secure service provisioning system for IoT using blockchain," Tech. Rep., 2021, doi: 10.21203/rs.3.rs-606120/v1.

[9] R. K. Shrivastava, V. Natu, and C. Hota, "Code integrity verification using cache memory monitoring," *Inf. Secur. J.: Global Perspective*, to be published, doi: 10.1080/19393555.2021.1902592.

[10] F. Ferdaus and M. T. Rahman, *Security of Emerging Memory Chips*. Cham, Switzerland: Springer, 2021.

[11] M. N. I. Khan and S. Ghosh, "Comprehensive study of security and privacy of emerging non-volatile memories," *J. Low Power Electron. Appl.*, vol. 11, no. 4, p. 36, 2021.

[12] D. M. Tank, A. Aggarwal, and N. K. Chaubey, "Cyber security aspects of virtualization in cloud computing environments: Analyzing virtualization-specific cyber security risks," in *Research Anthology on Privatizing and Securing Data*. Hershey, PA, USA: IGI Global, 2021, pp. 1658–1671.

[13] M. Saireddy, "Snoopy cache and shared memory model for commodity computing using cloud management system," *Ann. Romanian Soc. Cell Biol.*, vol. 25, no. 6, pp. 3902–3914, 2021.

[14] P. Gupta and N. K. Sehgal, "Information security and cloud computing," in *Introduction to Machine Learning in the Cloud With Python*. Cham, Switzerland: Springer, 2021, pp. 143–155.

[15] V. Krishnasamy and S. Venkatachalam, "An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using index-level boundary pattern convergent encryption algorithm," *Mater. Today: Proc.*, to be published, doi: 10.1016/j.matpr.2021.04.303.

[16] V. Sureshkumar and B. Baranidharan, "A study of the cloud security attacks and threats," in *Proc. J. Phys., Conf.*, 2021, vol. 1964, no. 4.

[17] M. M. Hossain, "Software security with hardware in mind," in *Emerging Topics in Hardware Security*. Cham, Switzerland: Springer, 2021, pp. 309–333.

[18] R. Agrawal, "Cache memory architecture for core processor," in *Proc. Int. Conf. Adv. Comput. Appl.* Singapore: Springer, 2022, pp. 809–820, doi: 10.1007/978-981-16-5207-3_66.

[19] R. Montasari, "Cloud computing security: Hardware-based attacks and countermeasures," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*. Cham, Switzerland: Springer, 2021, pp. 155–167.

[20] G. Sharma, G. Bousdras, S. Ellinidou, O. Markowitch, J.-M. Dricot, and D. Milojevic, "Exploring the security landscape: NoC-based MPSoC to cloud-of-chips," *Microprocessors Microsyst.*, vol. 84, Jul. 2021, Art. no. 103963.

[21] M. Srivastava, "An introduction to network security attacks," in *Inventive Systems and Control*. Singapore: Springer, 2021, pp. 505–515.

[22] A. Nyrkov, "Data structures access model for remote shared memory," in *Proc. E3S Web Conf.*, vol. 244, 2021, doi: 10.1051/e3sconf/202124407001.

[23] M. Esfahani, H. Soleimany, and M. R. Aref, "Enhanced cache attack on AES applicable on ARM-based devices with new operating systems," *Comput. Netw.*, vol. 198, Oct. 2021, Art. no. 108407.

[24] A. Hbaieb, S. Ayed, and L. Chaari, *Blockchain-Based Trust Management Approach for IoV*. Cham, Switzerland: Springer, 2021.

[25] Q. Xu, M. T. Arafin, and G. Qu, "Security of neural networks from hardware perspective: A survey and beyond," in *Proc. 26th Asia South Pacific Design Automat. Conf. (ASP-DAC)*, Jan. 2021, pp. 449–454.

[26] G. Christou, "The evolution of hardware-assisted security," in *Cybersecurity Issues in Emerging Technologies*. Boca Raton, FL, USA: CRC Press, 2021, pp. 1–20.

[27] L. H. Flå, "Tool-assisted threat modeling for smart grid cyber security," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment (CyberSA)*, Jun. 2021, pp. 1–8.

[28] E. Kafhali, I. E. M. Said, and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Arch. Comput. Methods Eng.*, vol. 29, pp. 223–246, Apr. 2021.

[29] Z. Sisi and A. Souri, "Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things," *Trans. Emerg. Telecommun. Technol.*, to be published, doi: 10.1002/ett.4217.

[30] W. Lu, L. Wu, R. Zhao, X. Li, and F. Xue, "Blockchain technology for governmental supervision of construction work: Learning from digital currency electronic payment systems," *J. Construct. Eng. Manage.*, vol. 147, no. 10, Oct. 2021, Art. no. 04021122.

[31] M. Khalil, K. F. Khawaja, and M. Sarfraz, "The adoption of blockchain technology in the financial sector during the era of fourth industrial revolution: A moderated mediated model," *Qual. Quantity*, to be published, doi: 10.1007/s11135-021-01229-0.

[32] W. Liang and N. Ji, "Privacy challenges of IoT-based blockchain: A systematic review," *Cluster Comput.*, to be published, doi: 10.1007/s10586-021-03260-0.

[33] J. Stodt, D. Schönle, C. Reich, F. Ghovanlooy Ghajar, D. Welte, and A. Sikora, "Security audit of a blockchain-based industrial application platform," *Algorithms*, vol. 14, no. 4, p. 121, Apr. 2021.

[34] S. Kumar, "Applying blockchain in agriculture: A study on blockchain technology, benefits, and challenges," in *Deep Learning and Edge Computing Solutions for High-Performance Computing*. Cham, Switzerland: Springer, 2021, pp. 167–181.

[35] Z. Zhou, M. Wang, J. Huang, S. Lin, and Z. Lv, "Blockchain in big data security for intelligent transportation with 6G," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 3, 2021, doi: 10.1109/TITS.2021.3107011.

[36] Q. Zhang, "Improving blockchain consistency by assigning weights to random blocks," Tech. Rep., 2021, doi: 10.48550/arXiv.2107.10467.

[37] M. Martin, "Power sector cybersecurity building blocks," Natl. Renew. Energy Lab NREL, Golden, CO, USA, Tech. Rep. NREL/TP-5R00-79396, 2021.

[38] S. Muralidhara and B. A. Usha, "Review of blockchain security and privacy," in *Proc. 5th Int. Conf. Comput. Methodol. Commun. (ICCMC)*, 2021, pp. 526–533, doi: 10.1109/ICCMC51019.2021.9418424.

[39] T. Gayvoronskaya and C. Meinel, "Technical basics for a better understanding of blockchain technology," in *Blockchain*. Cham, Switzerland: Springer, 2021, pp. 15–33, doi: 10.1007/978-3-030-61559-8_3.

[40] L. Bingzhang and V. Zirianov, "Blockchain in agricultural supply chain management," in *Proc. E3S Web Conf.*, vol. 273, 2021, doi: 10.1051/e3sconf/202127308029.

[41] A. Vispute, *Scaling Blockchain by Autonomous Sidechains*. Singapore: Springer, 2021.

[42] A. Srivastava, "Analyzing effects of architectural alternatives on performance of blockchain," in *Emerging Technologies in Data Mining and Information Security*. Singapore: Springer, 2021, pp. 943–956.

[43] A. Koltuksuz, "The biometric signature as a blockchain application," in *Blockchain Applications in IoT Ecosystem*. Cham, Switzerland: Springer, 2021, pp. 167–176.

[44] J. C. Kharbhih, K. P. Kalita, and R. K. Deka, "Integration of IoT and blockchain technology for smart cities," in *Emerging Technologies for Smart Cities*. Singapore: Springer, 2021, pp. 1–7, doi: 10.1007/978-981-16-1550-4_1.

[45] H. Doyu, R. Morabito, and M. Brachmann, "A TinyMLaaS ecosystem for machine learning in IoT: Overview and research challenges," in *Proc. Int. Symp. VLSI Design, Automat. Test (VLSI-DAT)*, Apr. 2021, pp. 1–5.

[46] N. Nikolov, O. Nakov and D. Gotseva, "Operating systems for IoT devices," in *Proc. 56th Int. Sci. Conf. Inf., Commun. Energy Syst. Technol. (ICEST)*, 2021, pp. 41–44, doi: 10.1109/ICEST52640.2021.9483469.

[47] A. A. Contractor, A. N. Banducci, and N. H. Weiss, "Critical considerations for the positive memory-posttraumatic stress disorder model," *Clin. Psychol. Psychotherapy*, vol. 29, no. 1, pp. 81–91, 2021.

[48] N. Islam, "Towards machine learning based intrusion detection in IoT networks," *Comput Mater Contin*, vol. 69, pp. 1801–1821, Mar. 2021.

[49] R. Ildar, "Increasing FPS for single board computers and embedded computers in 2021 (Jetson nano and YOVOv4-tiny). Practice and review," 2021, *arXiv:2107.12148*.

[50] C. Xu, Z. Liu, M. Liao, P. Li, Q. Xiao, and S. Yuan, "Fractional-order bidirectional associate memory (BAM) neural networks with multiple delays: The case of Hopf bifurcation," *Math. Comput. Simul.*, vol. 182, pp. 471–494, Apr. 2021.

[51] M. Atzenhoefer, "Business cards as a mechanism to encourage patient feedback about trainees," *J. Patient-Centered Res. Rev.*, vol. 8, no. 3, p. 267, 2021.

[52] H. Shafagh, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. Cloud Comput. Secur. Workshop*, 2017, pp. 45–50.

[53] R. Kaur and A. Ali, "Performance evaluation of secure blockchain framework for IoT based data communication," *Int. J. Syst. Assurance Eng. Manage.*, to be published, doi: 10.1007/s13198-021-01324-3.
[54] C. Gündoğan, "Content object security in the Internet of Things: Challenges, prospects, and emerging solutions," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 1, pp. 538–553, Mar. 2022.
[55] A. Cholakoska, M. Karanfilovska, and D. Efnusheva, *Survey of Security Issues, Requirements, Challenges and Attacks in the Internet of Things*. Cham, Switzerland: Springer, 2021.
[56] S. Birla, N. Singh, and N. K. Shukla, "Low-power memory design for IoT-enabled systems: Part 2," in *Electrical and Electronic Devices, Circuits and Materials*. Boca Raton, FL, USA: CRC Press, 2021, pp. 63–80.
[57] G. Prasad, "Process variation analysis of 10T SRAM cell for low power, high speed cache memory for IoT applications," in *Proc. 7th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Feb. 2020, pp. 891–895.
[58] M. Xie, C. Pan, Y. Zhang, J. Hu, Y. Liu, and C. J. Xue, "A novel STT-RAM-based hybrid cache for intermittently powered processors in IoT devices," *IEEE Micro*, vol. 39, no. 1, pp. 24–32, Jan. 2019.
[59] N. Gupta, "Sensing techniques," in *TFET Integrated Circuits*. Cham, Switzerland: Springer, 2021.
[60] T. S. Rani, "Low Power, High performance PMOS biased sense amplifier," in *Proc. 12th Int. Symp. Adv. Topics Elect. Eng. (ATEE)*, Mar. 2021, pp. 1–4.
[61] A. Johari and M. Panjwani, "Design and implementation of SRAM and DRAM cells, arrays and peripheral circuits," Tech. Rep. [Online]. Available: https://www.academia.edu/6578816/Design_and_implementation_of_SRAM_and_DRAM_Cells_Arrays_and_Peripheral_Circuits
[62] R. Agrawal, "Performance analysis of cache memory architecture for core processor," in *Control and Measurement Applications for Smart Grid*. Singapore: Springer, 2022, pp. 479–491, doi: 10.1007/978-981-16-7664-2_39.
[63] U. Nanda, D. Nayak, S. K. Saw, A. Majeed K K, and B. Jena, "Analysis of static noise margin of 10T SRAM using sleepy stack transistor approach," in *Proc. Devices Integr. Circuit (DevIC)*, May 2021, pp. 242–246.
[64] M. Gupta, K. Gupta, and N. Pandey, "Comparative analysis of the design techniques for low leakage SRAMs at 32 nm," *Microprocessors Microsyst.*, vol. 85, Sep. 2021, Art. no. 104281.
[65] R. Agrawal and V. K. Tomar, "Analysis of low power reduction techniques on cache (SRAM) memory," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–7.
[66] R. Agrawal, N. Faujdar, and A. Saxena, "Low power single-bit cache memory architecture," in *Proc. IOP Conf., Mater. Sci. Eng.*, 2021, vol. 1116, no. 1, Art. no. 012136.
[67] R. Agrawal and V. Goyal, *Analysis of MTCMOS Cache Memory Architecture for Processor*. Singapore: Springer, 2021.
[68] R. Agrawal, *Comparative Study of Latch Type and Differential Type Sense Amplifier Circuits Using Power Reduction Techniques*. Singapore: Springer, 2021.
[69] R. Agrawal and V. K. Tomar, "Analysis of cache(SRAM) memory for core i 7 processor," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–8.
[70] R. Agrawal and V. K. Tomar, "Implementation and analysis of low power reduction techniques in sense amplifier," in *Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Mar. 2018, pp. 439–444.
[71] S. Mittal, G. Verma, B. Kaushik, and F. A. Khanday, "A survey of SRAM-based in-memory computing techniques and applications," *J. Syst. Archit.*, vol. 119, Oct. 2021, Art. no. 102276.
[72] R. Banupriya, "Implementation of energy efficient BIST architecture by using verilog," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 2745–2750, 2021.
[73] D. Reis, M. Niemier, and X. S. Hu, "The implications of ferroelectric FET device models to the design of computing-in-memory architectures," *J. Integr. Circuits Syst.*, vol. 16, no. 1, pp. 1–8, Apr. 2021.
[74] S. Khan, "Performance analysis of 7 nm FinFET based 6t SRAM cell-transient and DC analysis," Ph.D. dissertation, Texas A&M Univ.-Kingsville, Kingsville, TX, USA, 2021.
[75] G. Ravikishore and N. M. Nandhitha, "6T-SRAM design to optimize delay using finfet technology," in *Proc. 3rd Int. Conf. Intell. Commun. Technol. Virtual Mobile Netw. (ICICV)*, Feb. 2021, pp. 540–544.
[76] V. Maddela, S. K. Sinha, and M. Parvathi, "Extraction of undetectable faults in 6T-SRAM cell," in *Proc. Int. Conf. Commun., Control Inf. Sci. (ICCISc)*, vol. 1, Jun. 2021, pp. 1–5.
[77] V. Harshey and S. K. Bansal, "Designing of variations tolerant sensing amplifier circuit for deep sub-micron memories," *ICTACT J. Microelectron.*, vol. 6, no. 4, pp. 1027–1033, 2021.
[78] C. Ryan and D. Foor, "Noise evaluation of various high-gain, very-low-noise current sense amplifier circuits," in *Proc. IEEE Aerosp. Conf.*, Mar. 2021, pp. 1–6.
[79] C. Duari, S. Birla, and A. K. Singh, "A 4×4 8T-SRAM array with single-ended read and differential write scheme for low voltage applications," *Semicond. Sci. Technol.*, vol. 36, no. 6, 2021, Art. no. 065013.
[80] R. Selvakumar, M. L. Kumar, and S. R. Gopal, "Material analysis of high degree of variability in thin CMOS for SRAM current sense amplifier," *Mater. Today: Proc.*, vol. 21, pp. 299–306, May 2020.
[81] T. Na, "Robust offset-cancellation sense amplifier for an offset-canceling dual-stage sensing circuit in resistive nonvolatile memories," *Electronics*, vol. 9, no. 9, p. 1403, 2020.