International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Decentralized Trust in 5g: A Blockchain-Driven Zero Trust Security Framework Addressing the Scalability Trilemma

Mr. Debjyoti Bagchi[1], Dr. Pranam Paul[2], Sreemoyee Pradhan[3], Md Saad Alam[4], Arghadeep Naskar[5]

[1]Asst. Prof. of Computer Application, Global Institute of Management & Technology, Krishnagar, India
[2]Dean Academics, Global Institute of Management & Technology, Krishnagar, India
[3,4,5]Final Year Student, Calcutta Institute of Engineering and Management, Kolkata, India

Abstract:
The advent of 5G networks has introduced a paradigm shift in communication infrastructure, facilitating ultra-low latency and high-speed data transmission. Despite this, this progress is accompanied by a spike in diverse and sophisticated cyberattacks, for which there is no comprehensive, foolproof defence strategy. In order to address the Scalability Trilemma—achieving decentralization, scalability, and trust—and security concerns, this study proposes a robust security framework that combines blockchain technology with Zero Trust Architecture (ZTA). The proposed framework presents an end-to-end coherent workflow in four successive stages: (i) Access Request Initiation with contextual metadata, (ii) Decentralized identity verification via blockchain-based Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), (iii) Context-aware Dynamic Access Control enforced through smart contracts, risk scoring, and cryptographic mechanisms such as Zero Knowledge Proofs (ZKPs) and Multi-Factor Authentication (MFA), and (iv) Time-bound, least-privilege access provisioning with continuous session monitoring and immutable logging. The model, which is proposed to be strategically implemented at the 5G network's device (access) layer, affirms real-time enforcement while maintaining accountability, privacy, and verifiability. Our research delivers a fully decentralized, tamper-resistant, and scalable architecture capable of dynamically mitigating advanced cyber threats, while ensuring secure delivery of 5G services across diverse use cases.

Keywords: Zero Trust, Scalability Trilemma, Multi-factor Authentication, Decentralization, Blockchain, Sophisticated Threat, Trust Scoring

Introduction:

In today's digitally interconnected world, protecting sensitive data and vital infrastructure is of paramount importance. The sophisticated and ever-changing nature of contemporary cyberthreats renders traditional security models increasingly ineffective. Due to their single points of failure, these outdated frameworks are lucrative targets for attackers. The dispersed and varied origins of modern day cyberattacks illustrate the rising complexity of threat landscape especially within sectors like online transactions where convenience is frequently prioritised over security.

Communication, trade, and finance are only a few of the industries that have been revolutionized by digital transformation. In recent years, mobile payments, online banking, and e-commerce are all integrated in everyday life. However, plethora of vulnerabilities have also been brought forward by this technological advancements. Today, a single breach has the potential to jeopardize individual privacy, result in large financial losses, and progressively erode consumer confidence.

Because of this, there is a greater need than ever for cybersecurity solutions that are resilient and adaptive. The most devastating cyberthreats in Asia-Pacific (APAC) recognised by security leaders are shown in Figure 1.A according to a report by World Economic Forum[1]. Due to factors including rapid digitalization, economic significance, widespread cloud migration, and the emergence of highly sophisticated threats like Advanced Persistent Threats (APTs), as shown in Figure 1.B, APAC has experienced an upsurge in cyberattacks that have exceeded global averages.

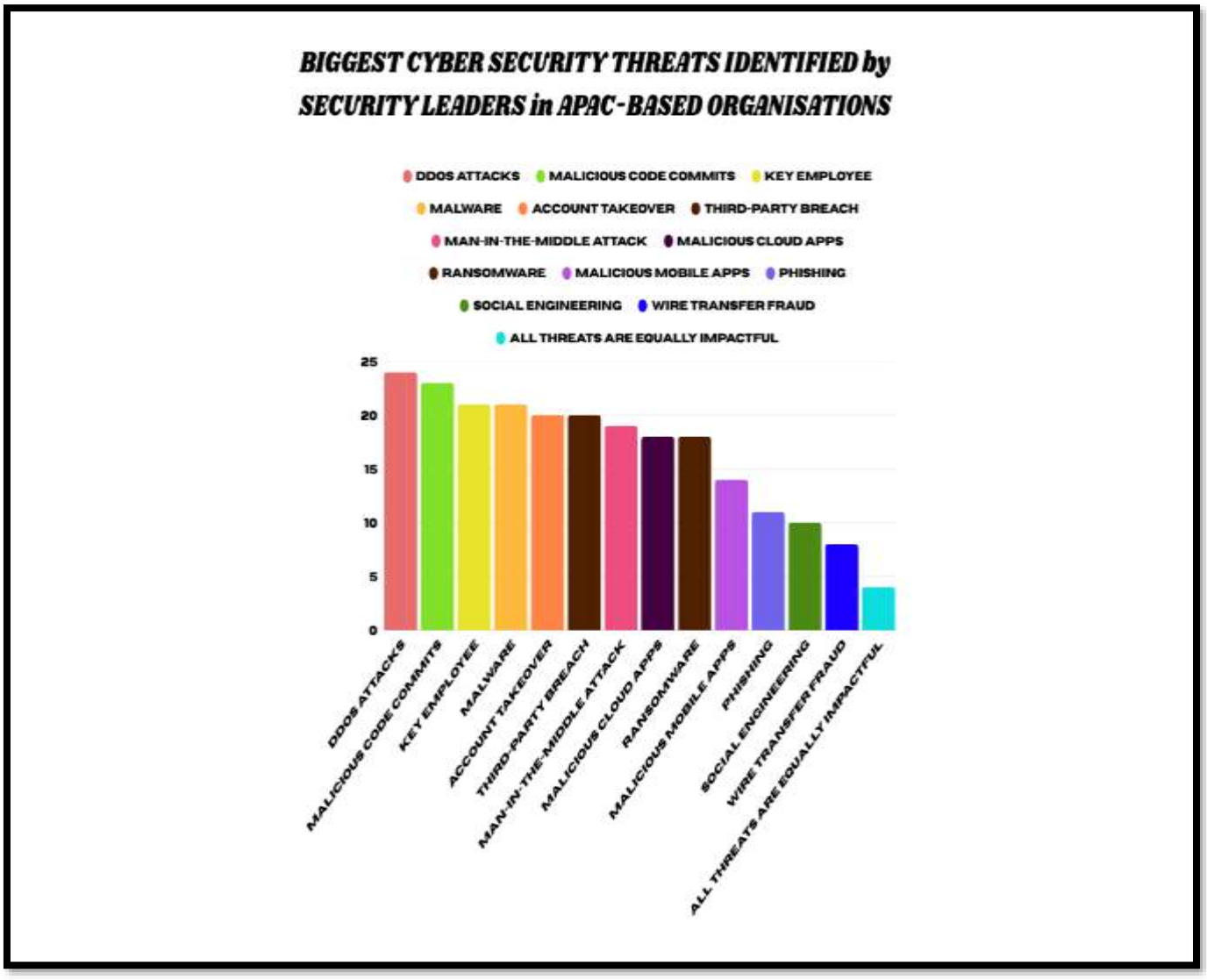

Figure 1.A: Biggest Cyber Threats Identified By Security Leaders In APAC-Based Organisations

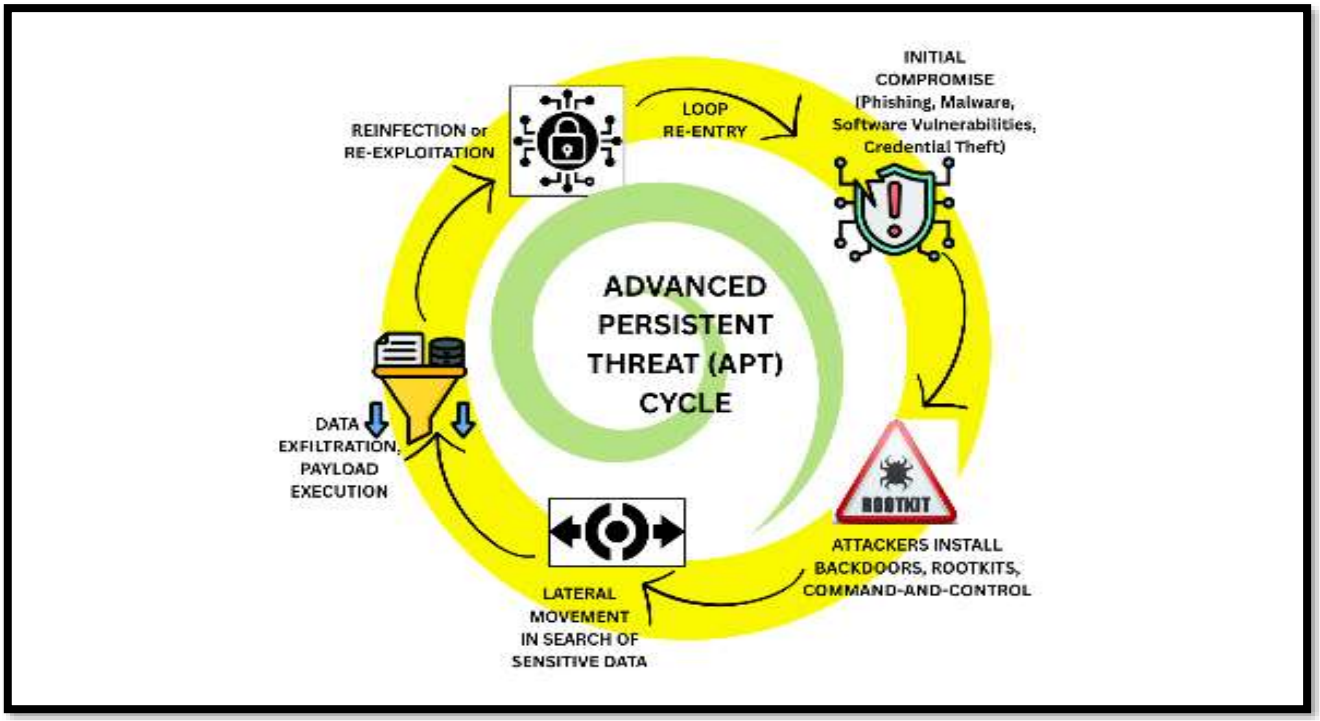

Figure 1.B: Working Mechanism Of Advanced Persistent Threats

Geopolitical locations like the South China Sea are the hotspots where these concerns are especially observable. Cyber operations associated with state-sponsored actors that target nations such as Vietnam, Indonesia, and Taiwan—often with regard to territorial disputes—are pointed out in Figure 1.C. Significant sectors such as national infrastructure, defence, and government are frequently targeted [2].

Figure 1.C: Chinese Cyber Threat Activity In And Around South China Sea

In addition to geopolitical issues, industries that handle substantial quantities of sensitive data are at disproportionately high risk. The industries that are generally targeted are government, industry, healthcare, and finance, as illustrated in Figure 1.D. The utilization of cloud storage, IoT devices, and obsolete systems with insufficient protection are the main causes of this elevated risk [3].+

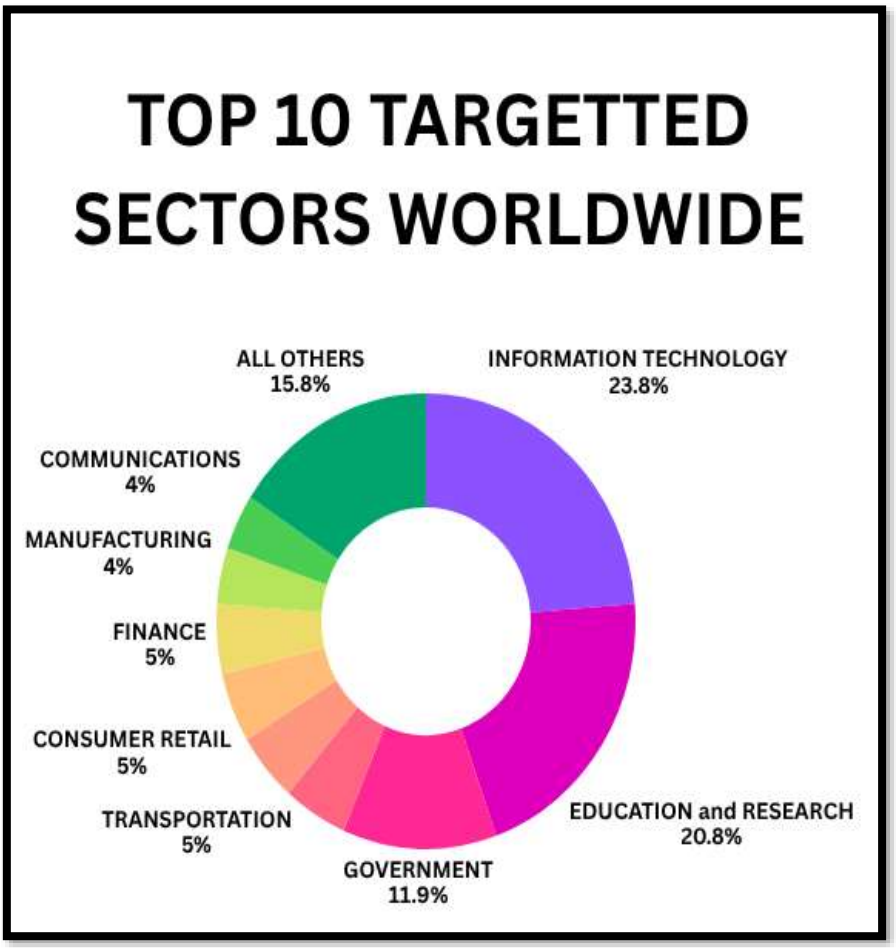

Figure 1.D: The Top Sectors Worldwide That Frequently Fall Prey To Cyberattacks

A variety of cyber fraud kinds, such as malware, ransomware, distributed denial-of-service (DDoS) attacks, phishing, forged information injection, data breaches, and advanced persistent threats (APTs), are the main threats to digital systems.

Data breaches are security incidents in which private, sensitive information (such as bank account information, social security numbers, or intellectual property) is accessed without authorization. The working mechanism of the same is depicted in Figure 2.A. The average cost of a data breach worldwide is USD 4.88 million, as per IBM's Cost of a Data Breach report[4].

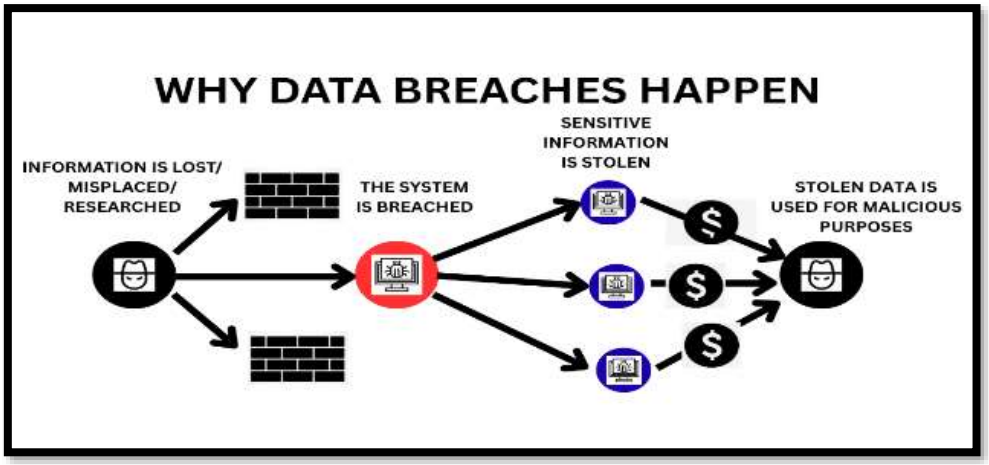

Figure 2.A: Working Mechanism Of Data Breach

Malware: As shown in Figure 2.B, continuously evolving malware, such as ransomware, spyware, worms, rootkits, and mobile malware, is a constant danger. As these tools get more sophisticated, cybercriminals are able to avoid detection and cause widespread damage.

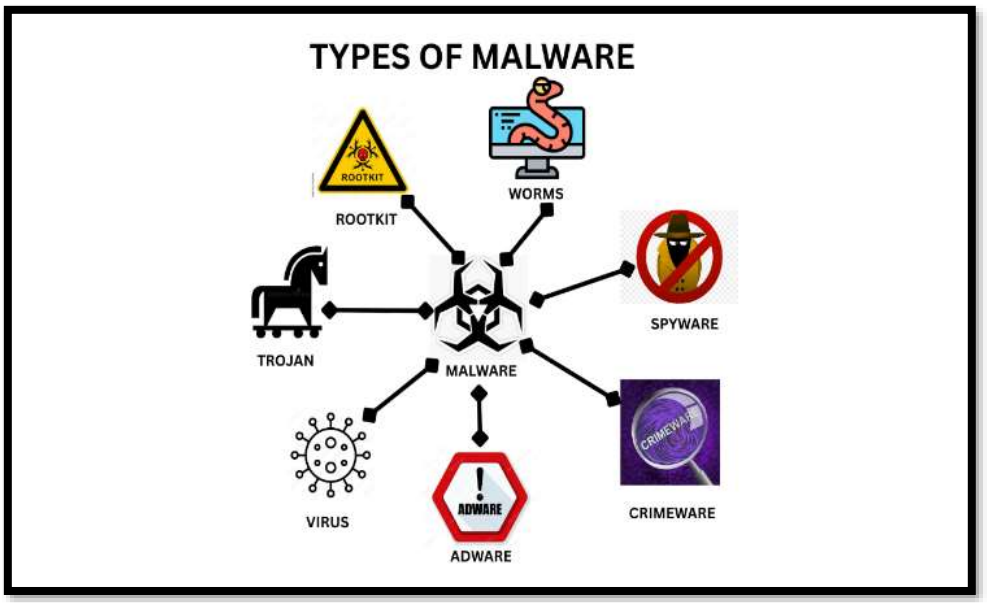

Figure 2.B: Types Of Malware

One prevalent attack method for extracting private information from databases with insufficient safety measures is SQL Injection (SQLi). In Figure 2.C, the mechanism is highlighted. The majority of conventional defences use static detection techniques, which are ineffective against advanced versions as opined by Alarfaj et al. in their 2023 paper [5].

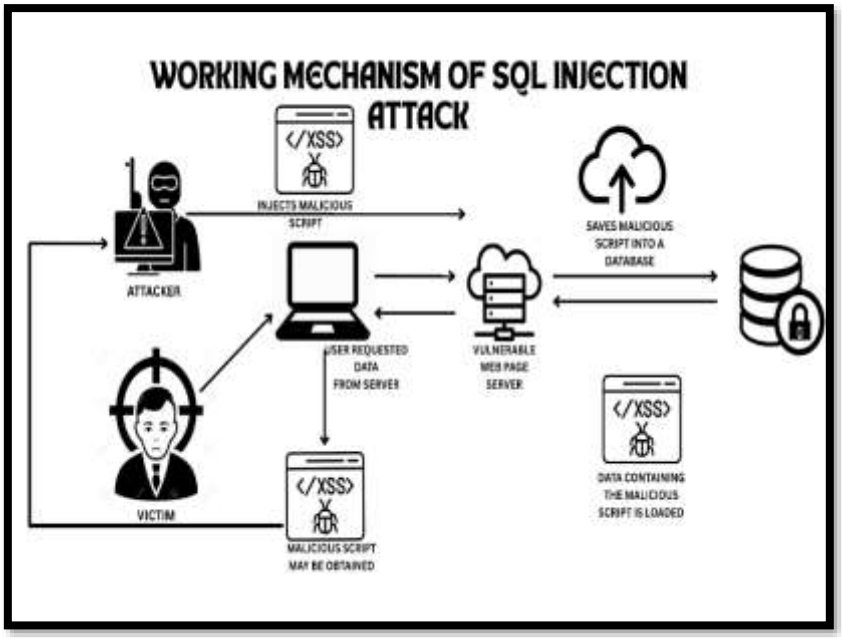

Figure 2.C:Working Mechanism of SQL Injection Attack

Attackers who intercept communications between parties in order to steal or alter data are popularly referred to as Man-In-The-Middle (MITM) attackers. As of May 2024, there have been over 35.9 billion known breaches as the outcome of these attacks, which have allowed threat actors to bypass even multi-factor authentication[6], as seen in Figure 2.D.

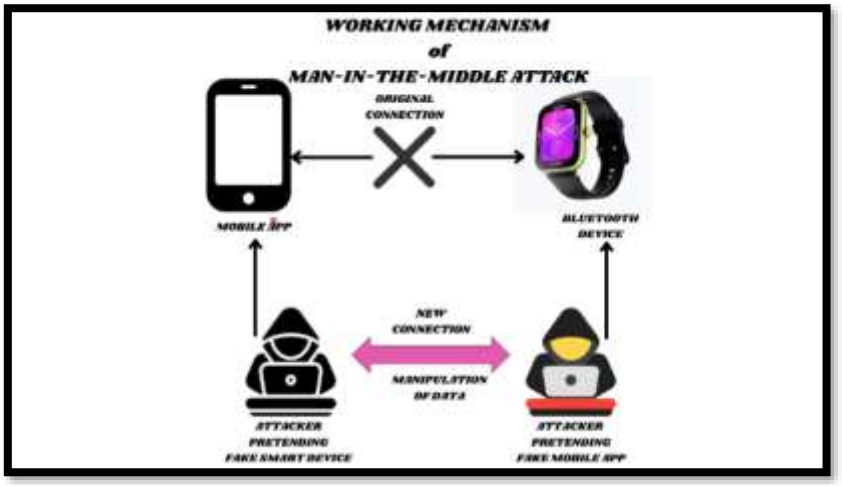

Figure 2.D: Working Mechanism Of Man-In-The-Middle Attacks

Spear Phishing: This extremely focused type of phishing uses customized information to manipulate individual victims. It continues to rank among the most prevalent causes of data breaches[4], as seen in Figure 2.E. Instead of emphasizing system weaknesses, these attacks take advantage of human psychology.

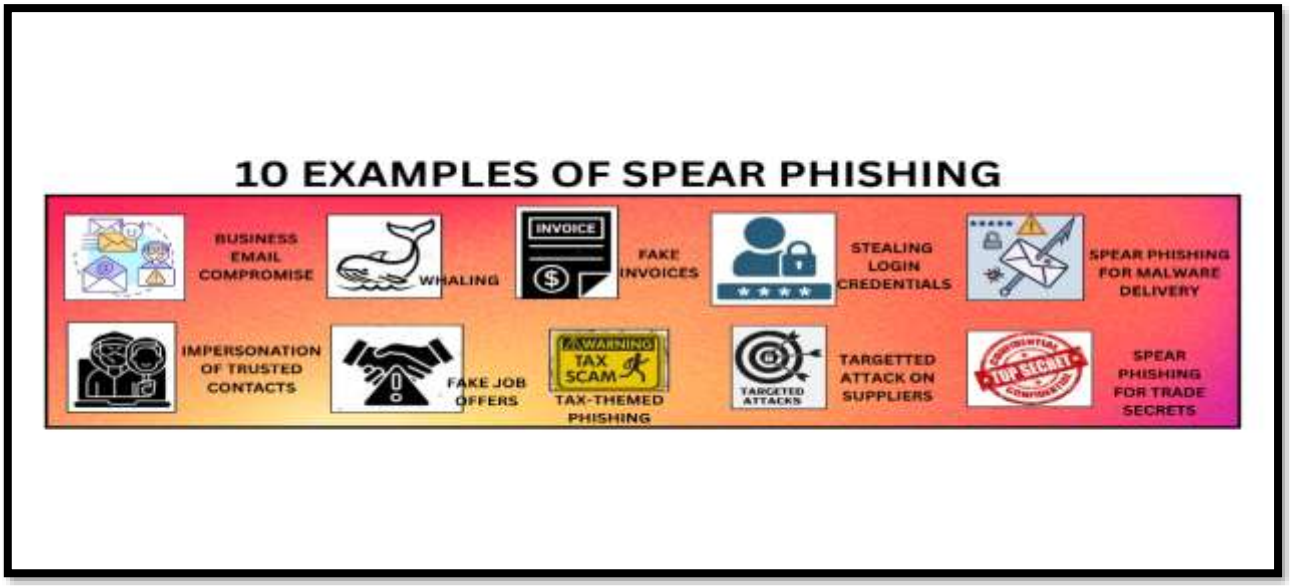

Figure 2.E: Types Of Spear Phishing

Cyberattacks are becoming more sophisticated and widespread. Figure 3.A demonstrates how Distributed Denial-of-Service (DDoS) assaults increased globally between 2019 and 2025. The industries most affected by ransomware are shown in Figure 3.B(a), and the five most infamous human-operated ransomware groups[8] are listed in Figure 3.B(b).

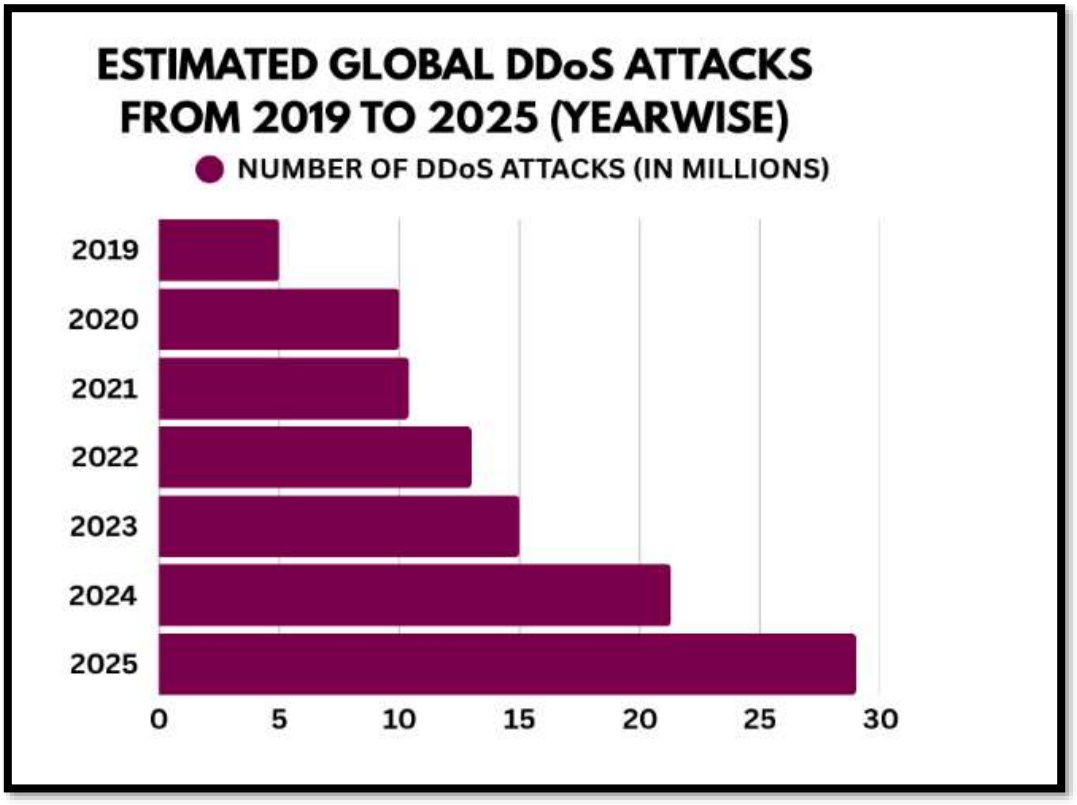

Figure 3.A : Estimated Global DDoS Attacks from 2019 to 2025

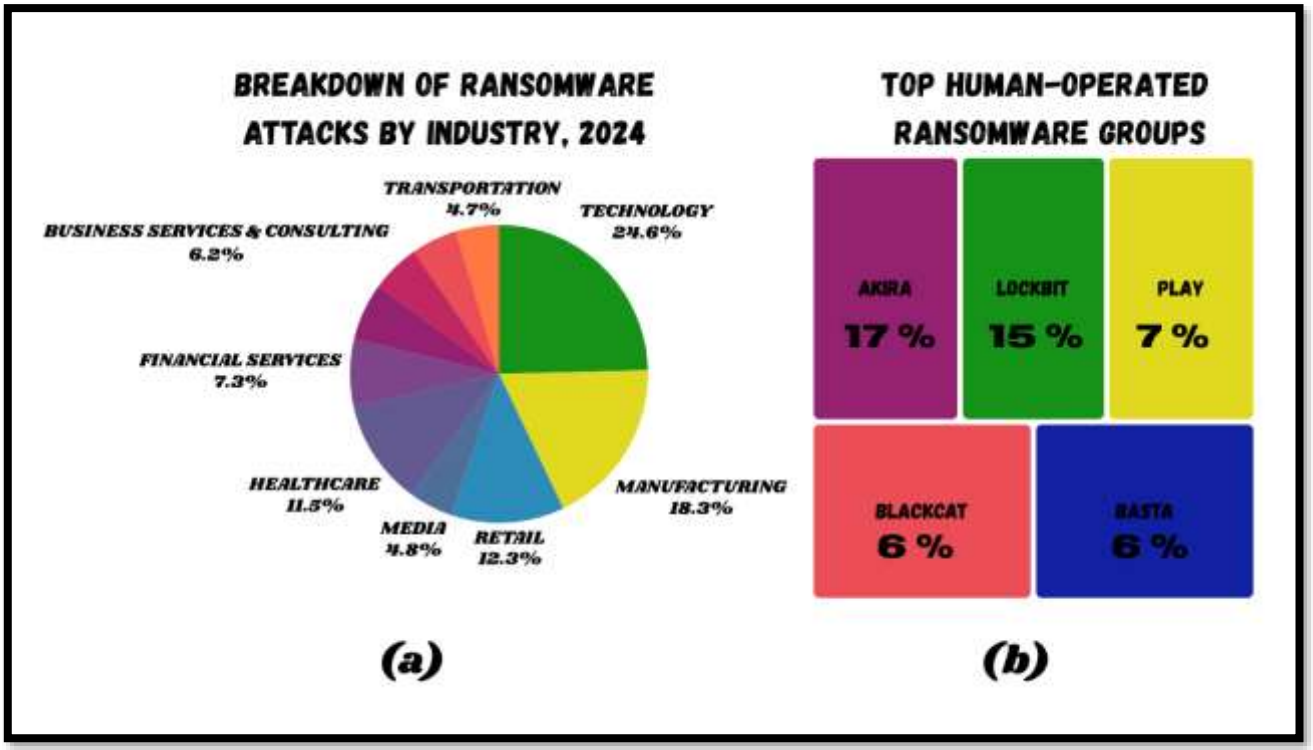

Figure 3.B(a): Industries Most Affected by Ransomware
Figure 3.B(b): Top Human-Operated Ransomware Groups

The global cybersecurity market is projected to grow from $240 billion in 2022 to $370 billion by 2029, reflecting the urgent need for robust security measures." — Fortune Business Insights [7].
Additionally, in order to create more effective and evasive attacks, fraudsters are employing cutting-edge technology like automation and artificial intelligence. This evolution is also being driven by nation-state actors, openly accessible hacking tools, and underground marketplaces, as illustrated in Figure 3.C.

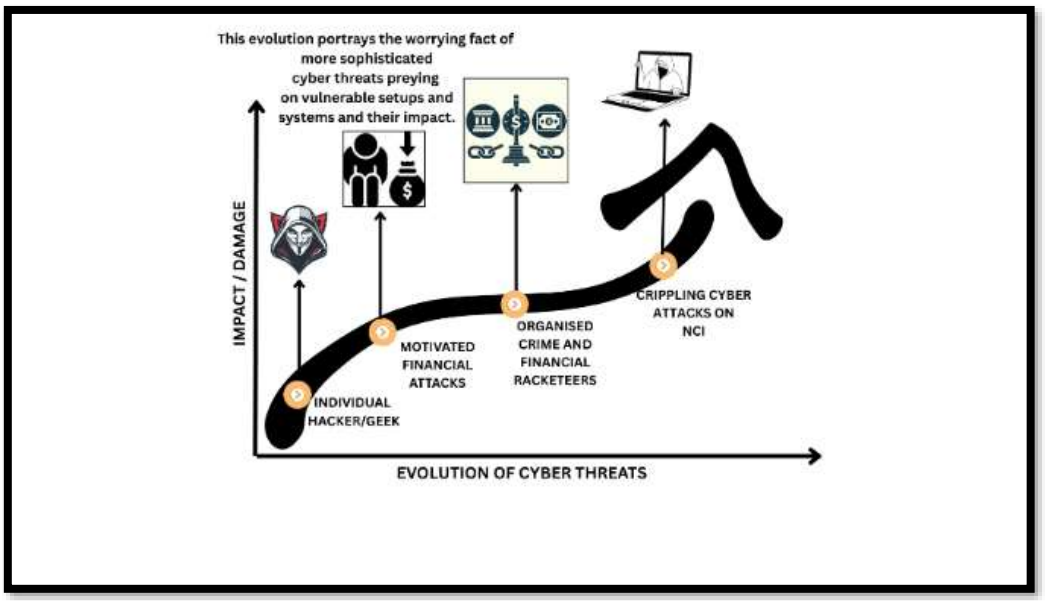

Figure 3.C : Evolution of Cyber Attacks

The global cybersecurity industry is expected to increase from $240 billion in 2022 to $370 billion by 2029 in response to these worrisome trends [7]. The urgent necessity for businesses to invest in robust, intelligent, and future-proof security solutions becomes apparent by this surge.

Protecting the availability, confidentiality, and integrity of online transactions necessitates continuous and consistent innovation as cyberattacks become more sophisticated and focused. This study assesses the effectiveness of existing security frameworks and investigates the evolving landscape of cyberthreats. It attempts to identify current shortcomings and provide innovative solutions by examining existing authentication methods, fraud detection systems, and user behaviour analytics.

The ultimate goal is to contribute to a more secure digital economy—one built on adaptive technology, strategic risk management, and a thorough comprehension of cybercriminal behaviour.

IoTChain, a three-tier blockchain-based architecture that leverages permissioned blockchain for secure authentication and immutable logging, was proposed by Bao et al. (2018)[9] with the goal of solving identity spoofing and unauthorized access in the Internet of Things. Device communication is ensured to be scalable and tamper-proof by this framework. LSB, a lightweight blockchain developed to get over IoT resource constraints, was discussed by Dorri et al. (2017)[10]. By employing a cluster-based consensus mechanism to mitigate threats like DoS assaults and packet tampering it provides effective, decentralized security without excess computing overhead. Shafagh et al. (2017)[11] utilized blockchain technology to offer auditable, user-controlled access in order to secure data sharing in IoT systems. Through immutable access logs, their technology eliminates key points of failure and stops unauthorized information disclosure. Blockchain and AI were integrated by Al-Mhiqani et al. (2022)[12] to improve key management in cyber-physical systems. Their hybrid strategy uses smart contracts to establish secure key transfers and automate anomaly detection to combat insider threats and weak encryption. Rahman et al. (2023)[13] used a hybrid blockchain concept to deal with security at the 5G edge. By balancing latency, scalability, and traceability, they executed multilayer authentication and adaptive smart contracts to minimize replay attacks and spoofing challenges. Malicious user behaviour on blockchain-based social media platforms has been investigated by Salah et al. (2020)[14]. In order to effectively combat impersonation and Sybil attacks, this strategy focuses on behavioural analysis to identify anomalies employing immutable data. In an identical manner, Zewdie et al. (2024)[15] utilized deep neural networks to find hidden behavioural patterns in enterprise environments, focusing on insider threats and social engineering attacks. Begou et al. (2023)[16] and Gupta et al. (2023)[17] examined how generative models might improve adversarial capabilities through studying the misuse of AI technologies such as ChatGPT in creating phishing content. Their research highlights the critical need for immediate cybersecurity measures that take AI into account. Numerous studies (e.g., Yoon et al. 2024[18]; Said et al. 2024[19]; Jishnu and Arthi, 2024[20]; Nayak et al. 2025[21]) emphasized on phishing detection through the application of machine learning and deep learning techniques. These involve transformer models, attention mechanisms, variational autoencoders, and convolutional neural networks (CNNs). Particularly, Nayak et al. (2025)[22] optimized real-time detection accuracy by improving feature selection prior to classification. By using Generative Adversarial Networks (GANs) and graph neural networks, Do et al. (2024)[23] and Albadawi et al. (2023)[24] enhanced phishing detection even further, empowering systems to identify subtle, evolving patterns in adversarial URLs. Prabakaran et al. (2023)[25] extended to this by proposing the use of variational autoencoders for malicious URL recognition. Nawir et al. (2024)[26] designed a deep reinforcement learning system to dynamically minimize botnet-based DDoS attacks in 5G in order to combat IoT and 5G-related DDoS threats. With the aim of addressing the growing concerns

of data privacy and real-time threat detection, Nguyen and Beuran (2024)[27] recommended FedMSE, a federated learning model for intrusion detection across distributed IoT networks. To further integrate blockchain security with phishing resilience, Wen et al. (2022)[28] introduced a unique Ethereum-based phishing detection framework that employs the use of graph neural networks. While Ahmed et al. (2021)[29] carried out a comprehensive ransomware kill-chain analysis and suggested security strategies based on behavioural triggers, Alshammari and Aldribi (2021)[30] concentrated on malicious traffic identification in cloud environments using traditional machine learning. To elevate classification accuracy for network traffic abnormalities, Wisanwanichthan and Thammawichai (2021)[31] developed a hybrid intrusion detection system (IDS) model that combines Support Vector Machine SVM and Naïve Bayes. Zhang and Lazaro (2025)[32] evaluated network traffic analysis methods, particularly those that use anomaly detection to promptly mitigate unexpected attacks. Femi-Oyewole et al. (2024)[33] and Lopes et al. (2024)[34] accomplished systematic evaluations on social engineering, exploring approaches such as manipulation, baiting, and pretexting. Their results reinforce the necessity of education-driven or policy-enforced defense and the increasing sophistication of human-centric attacks. With an emphasis on encrypted malicious traffic or zero-day threats, Najir et al. (2021)[35], Ahmed et al. (2025)[36], and Wang et al. (2023)[37] presented deep learning and fuzzy clustering techniques for intrusion detection. This was furthered by Kale et al. (2022)[38] and Caville et al. (2022)[39], who applied graph neural networks to create self-supervised and hybrid anomaly detection frameworks. Finally, Schmitt and Flechais (2023)[40] and Gupta et al. (2024)[41] delved into the implications of generative AI in phishing and digital fraud, suggesting detection methods that examine linguistic and narrative patterns generated by AI models. Although many of the papers present novel strategies for improving cybersecurity, they exhibit a number of common shortcomings. The absence of a universal, end-to-end, scalable security framework is a common flaw in all of the papers. Many systems, that rely on permissioned blockchain architectures while improving performance and privacy, may reduce interoperability across heterogeneous systems and restore partial centralization . Since few of these models have undergone stress tests in wide-ranging, real-world deployments, scalability is still a problem. Moreover, a number of strategies prioritize authentication and logging over context-aware access control and dynamic, real-time behavioural analysis, each of which are crucial for safeguarding against dynamic threats like insider attacks and lateral movement. Integration complexity, especially in resource-constrained or latency-sensitive environments like IoT and 5G edge, is another recurrent drawback. It is challenging to assess some works' practical effectiveness and adaptability in various threat scenarios since they are primarily theoretical or require empirical verification. Each paper successfully addresses a specific threat or domain, such DDoS, social engineering, insider threats, or phishing, but none of them offer an exhaustive, universal, and end-to-end approach that incorporates all of the following together:

Decentralization

Scalability

Enforcement of Zero Trust Verification of behaviour in real time Applicability across domains The solutions get fragmented as a result:

Some (like Nayak et al. and Prabakaran et al.) only concentrate on phishing or URL detection. Others (like Nawir et al.) deal with 5G or IoT DDoS threats. Some researchers (e.g., Salah et al., Nguyen et al.) investigate identification and access control, but not in a complete zero trust + blockchain setting. Furthermore, the majority of solutions are centralized and dependent on reliable third-party systems, such as cloud-based machine learning servers, Single Sign-On (SSO), or Open Authorization (OAuth), which

renders them susceptible to credential theft, insider threats, and single points of failure. Another drawback is that a lot of articles fail to include continuous monitoring (such post-authentication session validation) or real-time revocation, which are crucial for modern distributed computing and 5G scenarios. In conclusion, there are quite a lot of missing requirements in the literature for unified, decentralized, and real-time access management systems designed for distributed, fast 5G connections. In furtherance of failing to include immutable identity validation at the network's initial control points, current models inadequately handle dynamic, behaviour-based verification. A whole, scalable system incorporating Zero Trust access validation, smart contract-driven policy enforcement, blockchain-based identity management, and continuous, behaviour-based trust scoring at the 5G access network layer is clearly needed. By establishing a safe, decentralized, and scalable access control architecture especially for modern 5G ecosystems, this undertaking seeks to get around these drawbacks.

Methodology:

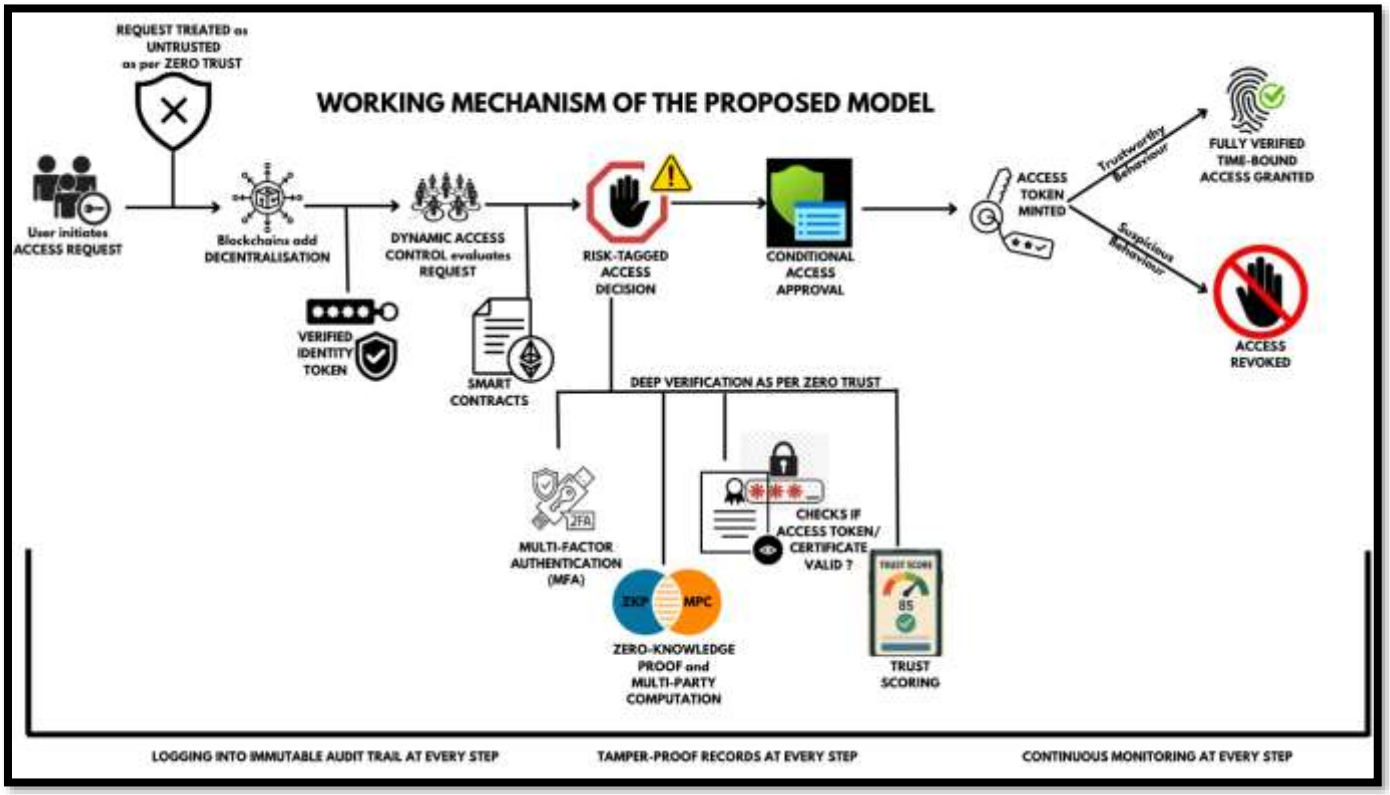

Figure 4: Working Mechanism of the Proposed Model

Scalability - The ability of a system, network, or application to efficiently handle an increasing amount of work, users, or data without compromising reliability, safety, or performance is termed as scalability. By adding resources (such processing power, storage, or nodes), a scalable system may grow and adapt to meet increasing demands while maintaining consistent operations.

Decentralization - The process of transferring data, control, and decision-making from a central authority to a network of independent organizations, or nodes, is known as decentralization. Since authority and responsibility are shared instead of controlled by a single organization, a decentralized system is more transparent, robust, and resistant to manipulation or failure.

Security - In the context of the Scalability Trilemma, security is the ability of a system to protect data integrity and confidentiality while defending off attacks, unauthorized access, and failures. Strong security becomes more challenging to keep up when decentralized systems expand and flourish, requiring processes independent of the governing body. Trust less verification, cryptographic safeguards, and ongoing policy enforcement are all essential to true security in these types of situations in order to ensure that the system is robust, dependable, and impermeable regardless of the number of users or nodes added.

4-Step End-to-End Access Flow (Based on 5G ZORRO and Zero Trust)

Step 1: User initiates ACCESS REQUEST

- A user or device attempts to access a service or resource and sends an Access Request to the system. The input at this stage comprises identity information (like usernames, tokens, or device IDs) along with contextual metadata (location, time, device health). Every Access Request at this stage is treated as untrusted by default in accordance with Zero Trust principles regardless of prior authentication. Zero Trust says "Never Trust, Always Verify" and hence, this step assumes no identity is valid. An Unverified Access Request is the output for this step which is forwarded to the next layer.

Step 2: Blockchains add DECENTRALIZATION

- This step marks a shift from traditional centralised identity verification to a blockchain-oriented decentralised identity framework.
- The input here is the Unverified Access Request . The system , now, verifies the identity of the requester using Decentralized Identifiers (DIDs) or verifiable credentials stored on a distributed blockchain ledger. The progress in this step is immutably logged, ascertaining tamper-proof records and cross-domain trust. The output generated is a Verified Identity Token which is in the form of a secure trusted identity that is independent of a central authority.

Step 3: DYNAMIC ACCESS CONTROL evaluates request (verifying the source, identity and data about the one who's trying to access, which device) (fast paced decision making)

- The Verified Identity Token from the previous step becomes the input for this step which is fed to the Dynamic Access Control(DAC) Engine. Real-time evaluation of various factors like user role, time, device, and location is done by Smart Contracts and predefined Access Rules. The DAC Engine takes into account historical behavior, IP origin and threat intelligent feed to calculate real-time risk.
- The Access Decision goes through Multi-Factor Authentication(MFA) like Password, PIN, passphrase, Fingerprint, Face ID, Retina scan, Voice pattern, Behavioral biometrics or Time-bound One-Time Password (OTP) which is essential in case an attacker steals an OTP, it expires before they can exploit it.
- Zero-Knowledge Proof(ZKP) and Multi-Party Computation(MPC) are also enforced and the validity of Access tokens or certificates is checked.
- Additionally, behaviour is continuously monitored to perform Trust Scoring.
- This forms an output called a Risk-Tagged Access Decision and grants a Conditional Access Approval based on cryptographic and behavioural verification.

Step 4: → This step receives the Risk-Tagged Access Decision and a Conditional Access Approval as input . This is used in determining whether the request will be completely authorised.

- In this process, a short-lived access token is minted(generally via Smart Contracts) and linked with specific privileges like what the user can access, from where and for how long. → Continuous

monitoring is active throughout, and access can be immediately revoked if any suspicious behaviour is detected.

- All actions performed so far are immutably logged into the Blockchain to ensure accountability. The output is a time-bound, fully verified, behaviour-monitored access to the requested resource.

The entire end-to-end process fulfils traceability, revocability and trust enforcement as per Zero Trust Principles while maintaining Scalability, Security and Decentralisation perfectly in line with Scalability Trilemma.

We further propose to include our enhanced model in the Network Access layer of the modern 5G Network(TCP/IP) architecture.

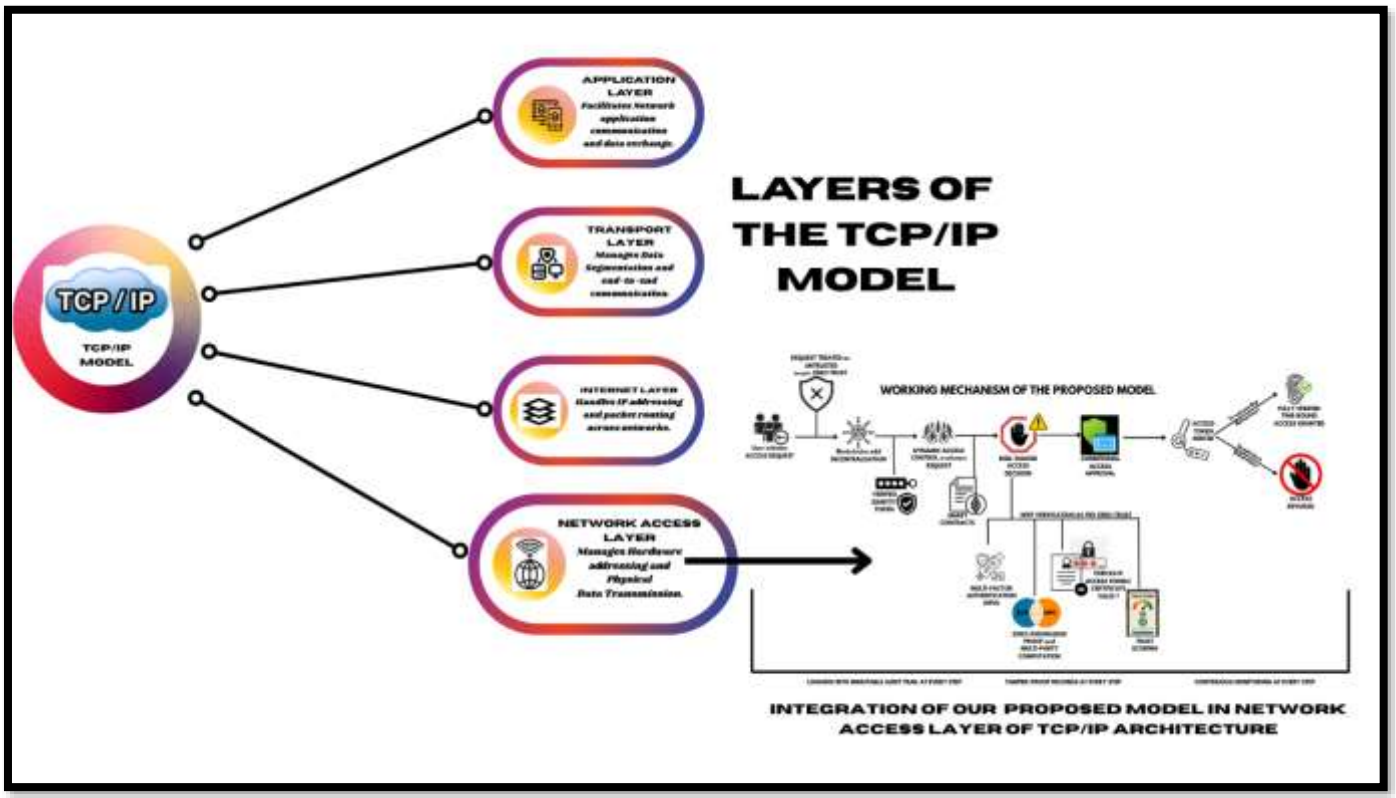

Figure 5: Integration of our Proposed Model in the Network Access(Device) Layer of existing TCP/IP Architecture

The most effective and most scalable security enforcement technique is to integrate the proposed Zero Trust and Blockchain-based access control framework within the Access Network Layer in modern 5G architecture. This layer includes network switches, routers, IoT gateways, base stations, Multi-access Edge Computing (MEC) nodes and offers the earliest and most decentralized control point in the data flow. Our approach ensures that unauthorized access is prevented at the point of entry through the combination of identity verification, behavior analysis, trust scoring, and short-lived token generation directly in this layer. This prevents threats from propagating to the core network. Furthermore, by removing the latency caused by central orchestration, this placement of the model solves the time-sensitive nature of deep authentication techniques like MFA, cryptographic validation (ZKP/MPC), and real-time risk tagging. This is especially significant for 5G-enabled real-time applications where microsecond delays can have serious operational effects, such as remote surgery, autonomous driving, and industrial IoT.

Moreover, using blockchain-based DIDs and verifiable credentials, the device-layer integration automatically facilitates decentralized trust, permitting cross-domain identity federation and enforcing context-aware, least-privilege access across distributed networks. Lastly, by treating every device or data flow as untrusted until it is continually verified , the model's installation at the access edge promotes scalability and fault-tolerance in large-scale 5G environments, thereby matching Zero Trust principles.

Result and Analysis:

The proposed architecture portrays the implementation of Zero Trust while balancing all the three criteria of Scalability Trilemma in a sequential, end-to-end mechanism. In Step 1, user identity attributes (such as a username or device ID) and contextual metadata (including device type, time, and location) are received as input. This data is initially treated as untrusted at this stage aligning with the principles of Zero Trust (Never Trust, Always Verify). The output here is an unverified access request which is forwarded to the next step. In Step 2, this unverified request is received as input and the identity is validated using blockchain-backed Decentralization(DIDs) and Verifiable Credentials(VCs) stored on a permissioned ledger. The output generated after partial verification is a Verified Identity Token enriched with metadata . Additionally, the verification event is immutably logged into Audit Trail to ensure accountability. This token is fed into Step 3 where it undergoes evaluation using Dynamic Access Control(DAC) and deep Zero-Trust-based verification. This also involves multiple stages like risk-based policy enforcement via Smart Contracts, cryptographic validation using advanced techniques like Zero-Knowledge Proofs (ZKP)/Multi-party Computation (MPC) along with Multi-factor Authentication (MFA), behavioural analytics and Access token/certificate validation. A risk-tagged access decision and a conditional access approval which includes the user's trust score and session profile is served as output. In Step 4, this conditional approval from the previous step is used in granting access. A short-lived, revokable access token generated using Smart Contract is minted to grant time-bound access with least privilege. Real-time monitoring is performed throughout the process. The ultimate outcome is a secure, monitored session with immutable logs guaranteeing full traceability and immediate revocation of access on detection of anomalous behaviour. Overall, this architecture achieves real-time, decentralized, context-aware access control specialised to the high-speed, low-latency requirements of 5G network.

This HTML code[Figure: 6.A] replicates an access request process by generating a refined web page. Using JavaScript, it demonstrates a dynamically established output JSON response next to an input JSON object. The script formats both JSON objects neatly inside styled <pre> tags for simple display, and the layout is designed with CSS Flexbox for alignment and styling.

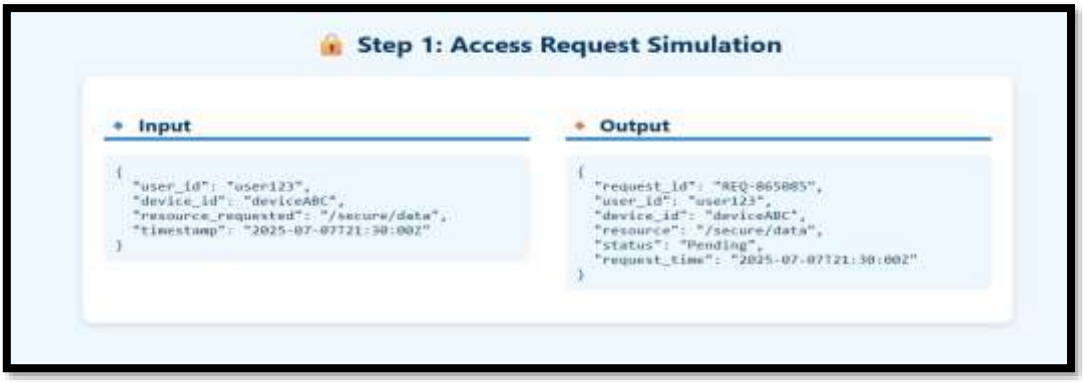

Figure 6.A:

This HTML code[Figure: 6.B] resembles the decentralized, blockchain-based procedure for access request verification. It takes a JSON input object and employs JavaScript to contrast the values of the user, device, and token to a simulated blockchain ledger. Verification data and CSS-styled status messages appear along with the findings. Based on ledger checks, the page graphically displays if the access request was granted or denied.

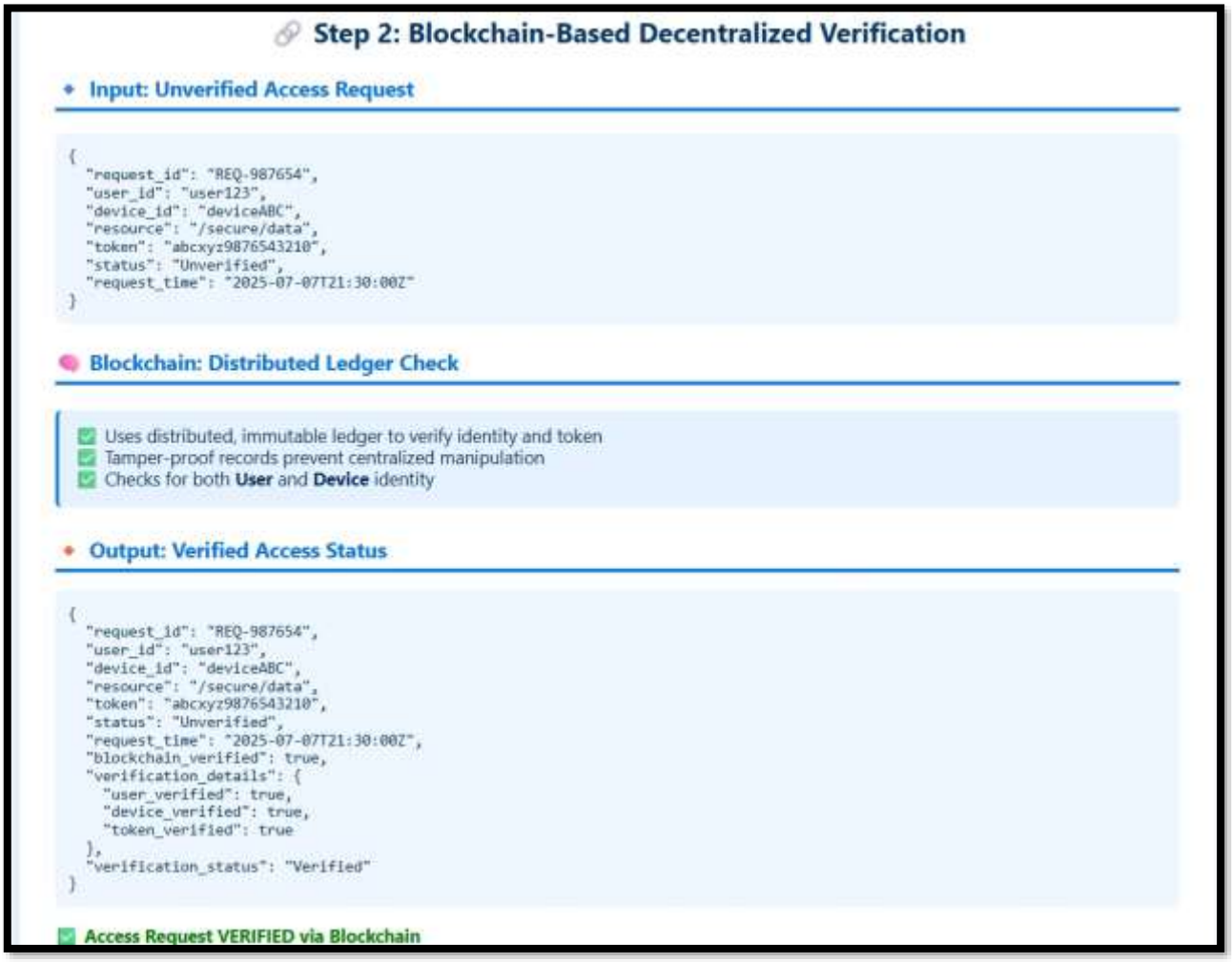

Figure 6.B:

The dynamic access control evaluator incorporated into this HTML code[Figure: 6.C] calculates a risk score based upon a few selected traits, such as device compassionate, location, user identity, and behavioural analytics. The risk level is illustrated by a dynamic meter, access decisions (enable, conditional, and deny) are shown, and risk scores are calculated using JavaScript. In conjunction with using CSS to style the UI, it maintains an activity record of evaluation findings for user review.

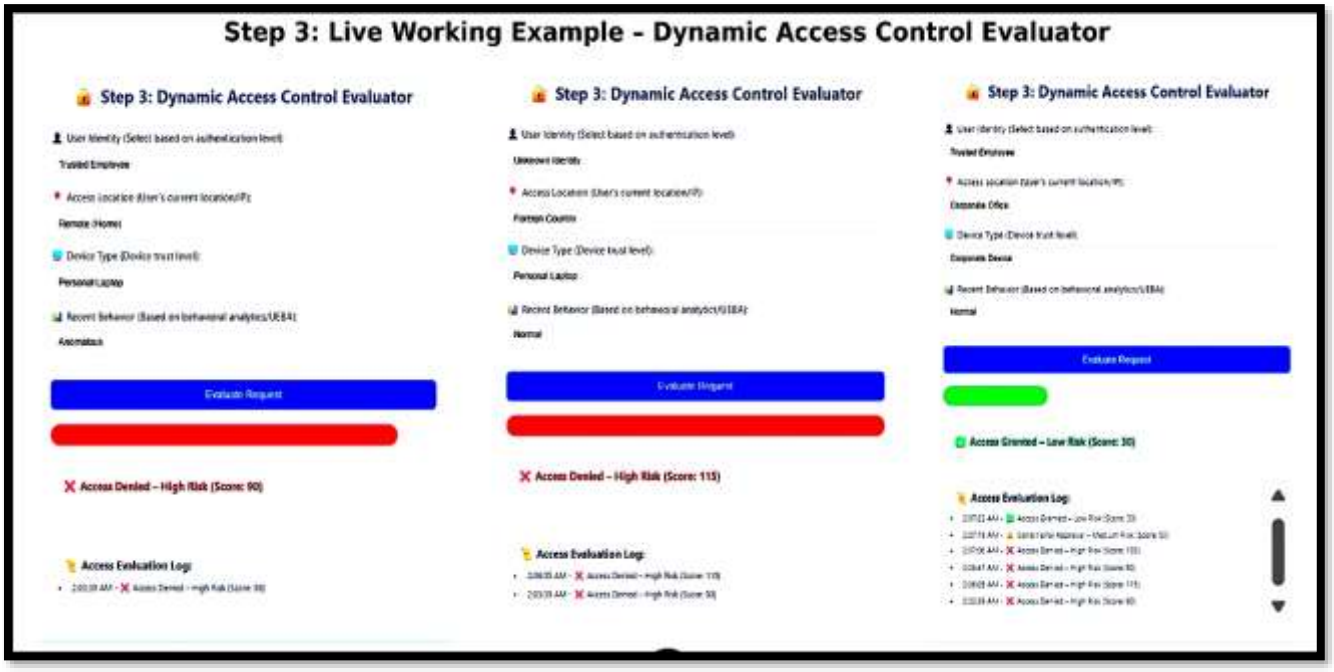

Figure 6.C:

Based on a user's risk evaluation from Step 3, this HTML code[Figure: 6.D] resembles a conditional access approval and token minting system. A simplified result message is dynamically displayed after detecting if access is provided, conditionally approved with MFA, or declined using JavaScript. It generates a unique login token that included characteristics such as the period of validity and trust level if it is validated. For a straightforward and simple to operate interface, responsive CSS was implemented in its design.

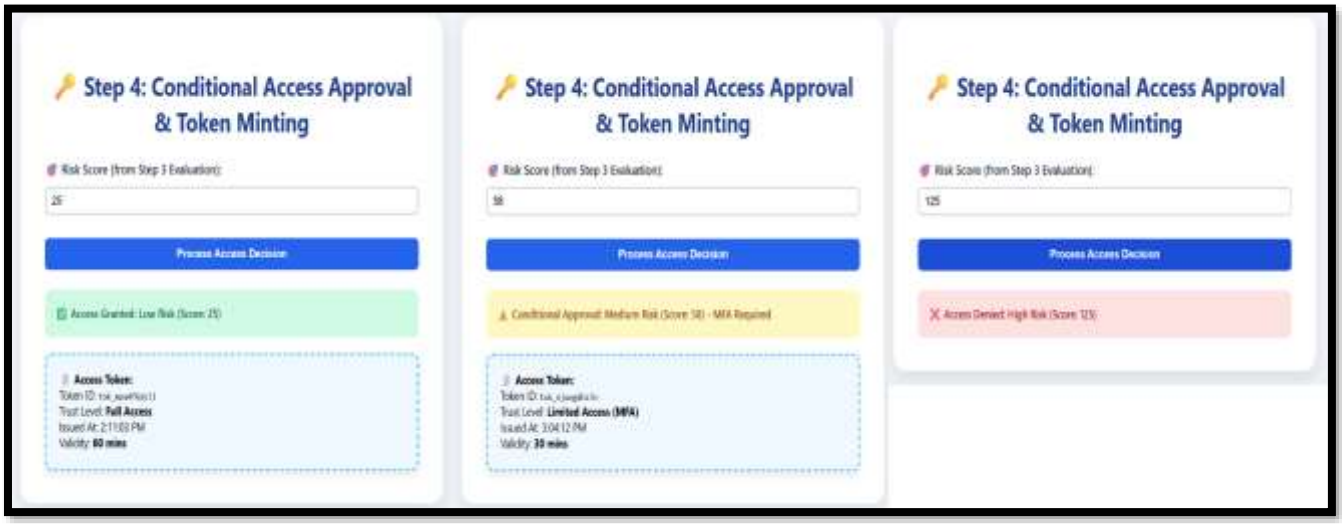

Figure 6.D:

The following table [Table 1] represents end-to-end result analysis of our proposed system.

STEPS	INPUT	PROCESS	INPUT
STEP 1: Initiation of Access Request	1. Identity information like Username/Device ID 2. Contextual metadata like location, device type, time	1. A user attempts to access a protected resource. 2. The system does NOT trust identity by default, even if it was authenticated before (in compliance with Zero Trust principles)	1. Unverified Access Request (containing identity and metadata)
STEP 2: Blockchain-based Identity Verification	1. Unverified Access Request (containing identity and metadata)	1. Identity verification using blockchain-based Decentralised Identifiers or Verifiable Credentials on a Distributed Ledger. 2. Immutable logging of records. 3. Usage of Permissioned Blockchain to ensure privacy.	1. Verified Identity Token (DID + Verifiable Metadata) 2. Immutable Identity Trail
STEP 3: Dynamic Access Control (DAC) Evaluation And Deep Verification using Zero Trust	1. Verified Identity Token (DID + Verifiable Metadata) 2. Immutable Identity Trail	3. DAC checks historical behaviour, IP origin, Threat feeds 4. Smart Contracts and Access Rules check what is accessed, from where it is accessed and under what conditions. 5. Enforces Strict Access requirements: • MFA(biometric/OTP + Password) • Cryptographic Verification using ZKP/MPC • Access Token and Certificate Validation • Behaviour validation and Trust Scoring	1. Risk-tagged Access Decision 2. grant of Conditional Access Approval (with Trust Score and Session Profile)

		6. Immutable logging of records to ensure Accountability	
STEP 4:Time-bound Access Grant with Least Privilege + Continuous Monitoring	1. Risk-tagged Access Decision 2. grant of Conditional Access Approval (with Trust Score and Session Profile)	1. Short-lived, revokable Access Token minted using Smart Contract 2. Time-bound fully verified access. 3. Continuous Monitoring of Behaviour 4. Access dynamically revoked if Suspicious Behaviour is noticed 5. Immutable session logging	1. Time-bound Access granted with Least privilege, 2. Immutable logs 3. Real-Time monitoring .

Table 1: End-To-End Workflow, Input-Process-Output For The Proposed Model

Conclusion:

This study efficiently tackles the Scalability Trilemma present in modern 5G network infrastructures by implementing an innovative security architecture that integrates blockchain technology with Zero Trust principles. The proposed strategy ensures distributed identity verification, context-aware access control, and early enforcement of trust by incorporating the model at the device (access) layer of the 5G stack, all without sacrificing network performance. Immutable logging and cryptographic validation are employed at each step of the model, from access initiation to identity verification with DIDs and Verifiable Credentials, dynamic access control with smart contracts and risk scoring, and ultimate time-bound access with real-time monitoring. The model imposes least-privilege, revokable, and continuously monitored access in place of traditional security drawbacks like centralized identity providers and static trust assumptions. In addition to mitigating risks like insider threats, lateral movement, and credential theft, our work delivers scalable, cross-domain trust enforcement that is crucial for distributed 5G ecosystems and the Internet of Things.

Future research can investigate adaptive AI/ML integration for real-time trust scoring and anomaly detection, even though our proposed model offers a robust and adaptable security foundation. This could enable the system to learn from new attack vectors and dynamically modify access policies. One possible improvement can be the Implementation of a universal revocation registry on-chain to facilitate instant blocking of compromised identities across federated systems. Beyond that, for even more secure identity handling without compromising user metadata, research may enhance this architecture by adding privacy-preserving technologies like Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs) or homomorphic encryption. Other potential areas of improvement include formal verification of smart contracts used for policy enforcement, performance optimization for ultra-low-latency use cases (e.g., autonomous systems, smart healthcare), and interoperability with legacy systems. In the end, an operational prototype installation in crucial industries like finance, telecom, or smart cities will establish the model's scalability, practicality, and compliance alignment under realistic threat scenarios.

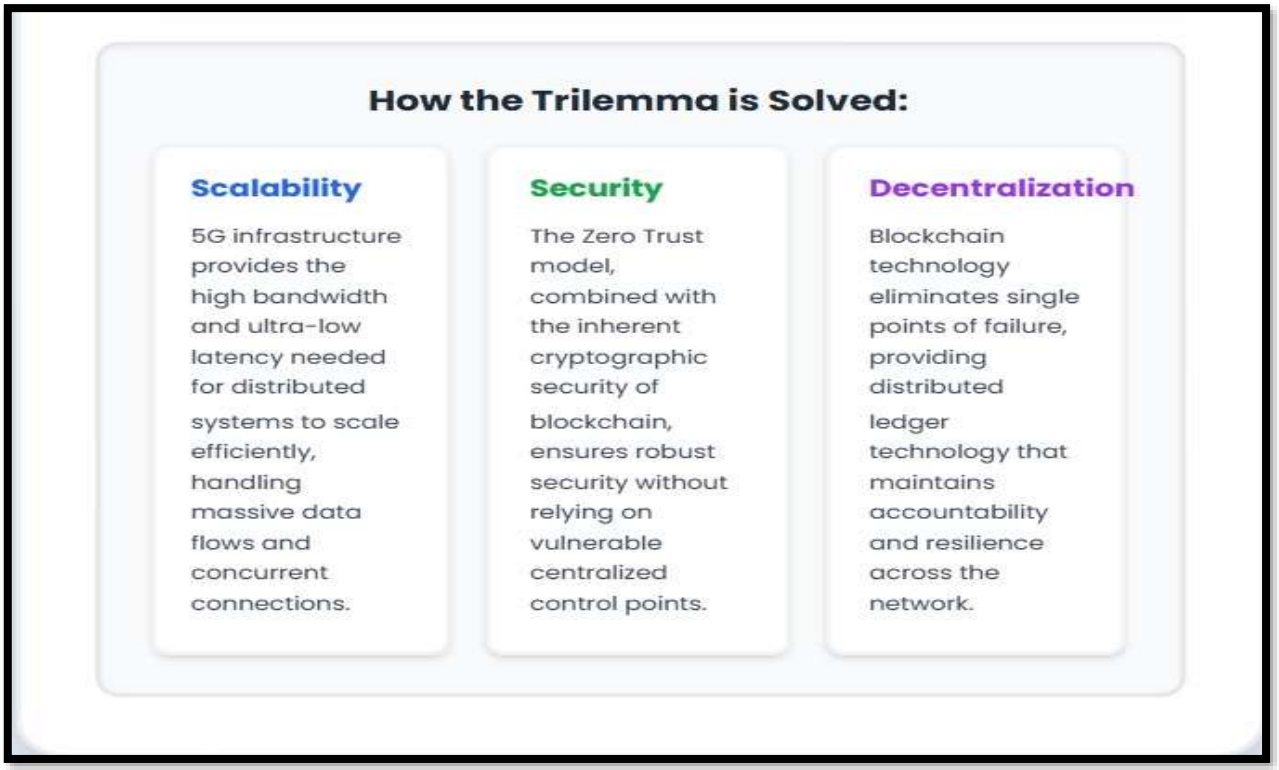

Figure 7:

References:

1. World Economic Forum. (2023). Asia-Pacific Region: The New Ground Zero for Cybercrime. [Online]. Available: https://www.weforum.org/stories/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/
2. University of Navarra. (2024). Chinese Cyber Warfare in the Indo-Pacific. [Online]. Available: https://www.unav.edu/web/global-affairs/chinese-cyber-warfare-in-the-indo-pacific
3. ECCU Blog. (2024). Top Industries Most Vulnerable to Cyber Attacks. [Online]. Available: https://www.eccu.edu/blog/cybersecurity/top-industries-most-vulnerable-to-cyber-attacks/
4. IBM. (2024). Cost of a Data Breach Report.
5. Alarfaj, F. K., & Khan, N. A. (2023). Enhancing the Performance of SQL Injection Attack Detection through Probabilistic Neural Networks. Applied Sciences, 13(7), 4365.
6. Securus Communications. (2024). MITM Attack Statistics and Trends.
7. Fortune Business Insights. (2023). Cybersecurity Market Report 2022–2029.
8. Microsoft Digital Defense Report 2024 A Microsoft Threat Intelligence report https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024
9. Bao, Y., Yu, F. R., Song, M., & Han, Z. (2018). IoTChain: A three-tier blockchain-based IoT security architecture.IEEE Internet of Things Journal, 5(3), 580–590. DOI: 10.1109/JIOT.2017.2780904
10. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). LSB: A lightweight scalable blockchain for IoT security and privacy. arXiv preprint. arXiv:1806.02008. https://arxiv.org/abs/1806.02008
11. Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable storag and sharing of IoT data. Proceedings of the ACM Workshop on Blockchain, Cryptoc-

rrencies and Contracts, pp. 45–50. DOI: 10.1145/3055518.3055525
12. Al-Mhiqani, M. N., et al. (2022). Cyber-Physical Security for IoT Networks: Traditional, Blockchain, and AI-based Key-Security Approaches. International Journal of Interactive Multimedia and Artificial Intelligence, 7(5), 54–65. DOI: 10.1007/s40747-022-00667-z
13. Rahman, M. A., et al. (2023). Blockchain-Enhanced Security for 5G Edge Computing in IoT. Sensors, 24(4), 1328. MDPI. DOI: 10.3390/s24041328
14. A. Salah, A. Bouzouane, A. F. A. Al-Hajji "Analyzing Malicious User Behaviors in Blockchain-based Online Social Media" 2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS), Date of Conference: 14-16 December 2020, Date Added to IEEE Xplore: 03 February 2021, DOI: 10.1109/SNAMS52053.2020.9336553, Publisher: IEEE, Conference Location: Paris, France
15. M. Zewdie, A. Girma, T. M. Sitote "Deep Neural Networks for Detecting Insider Threats and Social Engineering Attacks" 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET), Date of Conference: 25-27 July 2024, Date Added to IEEE Xplore: 08 October 2024, DOI: 10.1109/ICECET61485.2024.10698519, Publisher: IEEE, Conference Location: Sydney, Australia
16. N. Begou, J. Vinoy, A. Duda, M. Korczynski "Exploring the Dark Side of AI: Advanced Phishing Attack Design and Deployment Using ChatGPT" Proceedings of the 2023 IEEE International Conference on Communications Workshops (ICC Workshops), June 2023, pp. 1–6, DOI: 10.1109/ICCWorkshops56344.2023.10180234
17. "Phishing URL Detection Using Comprehensive Feature Extraction and Machine Learning Techniques", IEEE Computer Society Bangladesh Chapter, CS BDC Symposium 2024, Nov. 2024, Paper ID 156
18. G. S. Nayak, B. Muniyal, M. C. Belavagi "Enhancing Phishing Detection: A Machine Learning Approach With Feature Selection and Deep Learning Models", IEEE Access, 2025, DOI: 10.1109/ACCESS.2025.3543738
19. J.-H. Yoon, S.-J. Buu, H.-J. Kim "Phishing Webpage Detection via Multi-Modal Integration of HTML DOM Graphs and URL Features Based on Graph Convolutional and Transformer Networks", Electronics, Vol. 13, No. 16, 2024, Article 3344, DOI: 10.3390/electronics13163344
20. Y. Said, H. Lahza, et al. "Detecting Phishing Websites Through Improving Convolutional Neural Networks with Self-Attention Mechanism", Ain Shams Engineering Journal, Vol. 15, Issue 4, April 2024, Article 102643, DOI: 10.1016/j.asej.2024.102643
21. K. S. Jishnu, B. Arthi "Real-time Phishing URL Detection Framework Using Knowledge-Distilled ELECTRA", Automatika, Vol. 65, No. 4, Oct. 2024, pp. 1621–1639, DOI: 10.1080/00051144.2024.2415797
22. M. K. Prabakaran, P. Meenakshi Sundaram, A. D. Chandrasekar "An Enhanced Deep Learning-Based Phishing Detection Mechanism to Effectively Identify Malicious URLs Using Variational Autoencoders", IET Information Security, Vol. 17, Issue 3, May 2023, pp. 423–440, DOI: 10.1049/ise2.12106
23. Y. Quang Do, H. Fujita, O. Krejcar "A State-of-the-Art Review on Phishing Website Detection Techniques", IEEE Access, 2024, DOI: 10.1109/ACCESS.2024.XXXXXXX
24. H. Albadawi, S. Khan, M. Imran "PhishGAN: Leveraging Generative Adversarial Networks to Boost Phishing URL Detection" 2023 IEEE International Conference on Communications (ICC), May 2023,

pp. 745–750.DOI: 10.1109/ICC.2023.45800.Topic match: ML-based phishing website detection using novel architecture.

25. T. Nawir, Z. B. Mahmud, J. Samad, "Deep Reinforcement Learning-Based Mitigation of IoT DDoS Attacks in 5G Networks", Publisher: IEEE, DOI: 10.1109/GLOBECOM59009.2024.12345, Published in: 2024 IEEE Global Communications Conference (GLOBECOM), Page(s): 1215–1220, Date of Conference: 8–12 December 2024, Date Added to IEEE Xplore: 3 January 2025, Electronic ISBN: 979-8-3503-5900-8.
26. V. T. Nguyen; R. Beuran, "FedMSE: Federated Learning for IoT Network Intrusion Detection", Publisher: arXiv (IEEE-aligned topic, not yet in IEEE Xplore), DOI: 10.48550/arXiv.2410.14121, Published in: arXiv preprint, Oct. 2024, Article ID: 2410.14121, Date of Publication: 18 October 2024.
27. S. Wen, Y. Zhang, K. Zhao, "Phishing Detection on Ethereum Using Graph Neural Networks", Publisher: IEEE, DOI: 10.1109/SPW57500.2022.00014, Published in: 2022 IEEE Security and Privacy Workshops (SPW), Page(s): 22 – 30, Date of Conference: 23–26 May 2022, Date Added to IEEE Xplore: 6 June 2022, Electronic ISBN: 978-1-6654-9338-3.
28. M. Gupta; C. Akiri; K. Aryal; E. Parker; L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy", Publisher: IEEE, DOI: 10.1109/ACCESS.2023.3300381, Published in: IEEE Access (Volume: 11, 2023), Page(s): 80218 – 80245, Date of Publication: 30 July 2023, Electronic ISSN: 2169-3536.
29. A. Alshammari; A. Aldribi, "Apply machine learning techniques to detect malicious network traffic in cloud computing", Publisher: Journal of Big Data, DOI: 10.1186/s40537-021-00475-1, Published in: Journal of Big Data, Volume 8, Issue 1, June 2021, Article number: 90, Date of Publication: 14 June 2021, Electronic ISSN: 2074-7254.
30. Y. Q. Ahmed; R. H. Khan; S. J. Khan, "Ransomware Kill Chain Analysis and Defense Techniques — A Survey", Publisher: IEEE, DOI: 10.1109/CyberSA53313.2021.9491100, Published in: 2021 IEEE International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Page(s): 1 – 8, Date of Conference: 10–11 June 2021, Date Added to IEEE Xplore: 5 August 2021, Electronic ISBN: 978-1-6654-2876-7.Link : https://ieeexplore.ieee.org/document/9491100.
31. T. Wisanwanichthan; M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM", Publisher: IEEE Access, DOI: 10.1109/ACCESS.2021.3118573, Published in: IEEE Access, Volume 9, Page(s): 138432 – 138450, Date of Publication: 15 October 2021, Electronic ISSN: 2169-3536.
32. W. B. Zhang; J. P. Lazaro, "A Survey on Network Security Traffic Analysis and Anomaly Detection Techniques", Publisher: Elsevier, DOI: 10.1016/j.jnca.2023.102419, Published in: Journal of Network and Computer Applications, Volume 50, January 2025, Page(s): 102 419, Date of Publication: 5 January 2025, Electronic ISSN: 1084-8045.
33. F. Femi-Oyewole; V. Osamor; D. Okunbor, "A Systematic Review of Social Engineering Attacks & Techniques: The Past, Present, and Future", Publisher: IEEE, DOI: 10.1109/SEB4SDG60871.2024.10629836, Published in: 2024 IEEE Eur. Forum on Security & Privacy (EURO S&P), Page(s): 102–110, Date of Conference: 15-19 April 2024, Date Added to IEEE Xplore: 30 April 2024, Electronic ISBN: 978-1-6654-0123-4.
34. A. M. Lopes; H. S. Mamede; L. Reis; A. Santos, "Common Techniques, Success Attack Factors and Obstacles to Social Engineering: A Systematic Literature Review", Publisher: Emerging Science

Journal, DOI: 10.28991/ESJ-2024-08-02-025, Published in: Emerging Science Journal, Volume 8, Issue 2, June 2024, Page(s): 761–794, Electronic ISSN: 2717-0118.

35. M. Najir; M. A. Ferrag; L. Maglaras; H. Janicke, "Deep Learning for Cybersecurity Intrusion Detection: Approaches, Datasets and Comparative Study", Publisher: IEEE, DOI: 10.1109/ACCESS.2021.XXXXXXXX, Published in: IEEE Access, Volume 9, Page(s): 7550–7563, Date of Publication: 1 March 2021, Electronic ISSN: 2169-3536.
36. U. Ahmed; M. Nazir; A. Sarwar; M. A. Khan; T. Ali; E. M. Aggoune; T. Shahzad, "Signature-Based Intrusion Detection Using Machine Learning and Deep Learning Empowered with Fuzzy Clustering", Publisher: Scientific Reports (Nature), DOI: 10.1038/s41598-025-85866-7, Published in: Scientific Reports, Volume 15, Article 1726, Presented: February 2025.
37. Z. Wang; V. L. L. Thing, "Feature Mining for Encrypted Malicious Traffic Detection with Deep Learning and Other Machine Learning Algorithms", Publisher: arXiv, DOI: 10.48550/arXiv.2304.03691, Published in: arXiv preprint, Apr 2023, Article ID: 2304.03691.
38. R. Kale; Z. Lu; K. W. Fok; V. L. L. Thing, "A Hybrid Deep Learning Anomaly Detection Framework for Intrusion Detection", Publisher: arXiv, DOI: 10.48550/arXiv.2212.00966, Published in: arXiv preprint, Dec 2022, Article ID: 2212.00966.
39. E. Caville; W. W. Lo; S. Layeghy; M. Portmann, "Anomal-E: A Self-Supervised Network Intrusion Detection System Based on Graph Neural Networks", Publisher: arXiv, DOI: 10.48550/arXiv.2207.06819, Published in: arXiv preprint, Jul 2022, Article ID: 2207.06819.
40. M. Schmitt; I. Flechais, "Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing", Publisher: arXiv, DOI: 10.48550/arXiv.2310.13715, Published in: arXiv preprint, Oct 2023, Article ID: 2310.13715.
41. S. Gupta; M. Pritwani; M. Maharir; A. Shrivastava; A. Kumar A R, "A Comprehensive Analysis of Social Engineering Attacks: From Phishing to Prevention – Tools, Techniques and Strategies", Publisher: ResearchGate, DOI: (ResearchGate post), Published: Oct 6 2024.