ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14621435

Next-Generation Defense Security: Blockchain, IoT, Digital Twin, and Face Recognition-Based Smart Monitoring System

Priya.M[1]; Viji.K[2]
Assistant Professor[1]; Student[2]
Department of Computer Science and Engineering, Tagore
Institute of Engineering and Technology ,
Deviyakuruchi, Salem, Tamil Nadu, India

Abstract:- Protecting sensitive data, personnel, and assets in the defence sector against unauthorised access and security breaches requires authentication. Strong authentication protocols are needed to preserve the security and integrity of military networks, systems, and facilities as defence operations become more digitalised. The development of safe and efficient monitoring systems is necessary due to the quick advancements in technology and the increasing complexity of defence operations. This article addresses the unique security issues faced by the military industry by combining blockchain technology, AI-powered facial recognition technology, and Internet of Things-based digital twin technology. The proposed system builds a robust platform for monitoring people, assets, and critical infrastructure by utilising blockchain's inherent advantages, including decentralisation, immutability, and enhanced security. By employing facial recognition technology to instantly identify and validate people, the system automates access control and grants only authorised individuals access to vital resources or restricted areas. To prevent manipulation and safeguard data privacy, licensed workers' biometric information is safely stored on the blockchain. The decentralised ledger records each access attempt, permitted or not, establishing an unchangeable audit trail for compliance and accountability. Blockchain-integrated smart contracts enable automated responses to security incidents, like alerting authorities, setting off alarms, or securing areas when unauthorised individuals are detected. The distributed form of the framework eliminates single points of failure, boosting defences against upcoming cyberattacks and guaranteeing business continuity.

Keywords:- *Authentication, Block Chain, Digital Twin Technology, Face Recognition, Monitoring Systems, Smart Contracts, Security Branches, Unauthorised Access.*

I. INTRODUCTION

A sophisticated database approach called blockchain technology makes it possible for transparent information to be shared across a corporate network. Data is stored in blocks that are linked together in a chain within a blockchain database. Since network consensus is required to remove or alter the chain, the data is chronologically consistent. Blockchains function as a public distributed ledger and are frequently managed using peer-to-peer (P2P) computer networks. Nodes create and validate new transaction blocks using a consensus method protocol. Blockchains may be said to as secure by design, illustrating a distributed computing system with great Byzantine fault tolerance, even though blockchain records are not unchangeable due to the possibility of blockchain forks. Conventional database solutions have a number of challenges when it comes to recording financial transactions. Think about the sale of a home. The buyer receives possession of the property after the money is transferred. Both the seller and the buyer can independently record financial transactions, but neither source is trustworthy. The customer can assert that they have paid the money when they haven't, and the vendor can simply state that they haven't received it when they have. Transactions must be monitored and verified by a reliable third party to avoid any legal issues. This central authority creates a single point of risk and complicates the process. Both parties can suffer if the central database is compromised. By creating a decentralised, impenetrable system for transaction recording, blockchain overcomes these challenges. Blockchain creates a single ledger for each buyer and seller in a real estate transaction. Every transaction is automatically entered in both ledgers in real time and requires both parties' approval. The ledger as a whole will be impacted by any corruption in previous transactions. Because of these characteristics, blockchain technology has been used in many other fields, including the creation of virtual currencies like Bitcoin. The scope of the study includes developing and implementing a state-of-the-art security framework designed to satisfy the complex requirements of contemporary defence systems. By removing the limitations of outdated methods like ID cards and passwords, it focusses on implementing robust access control through the use of contemporary facial recognition technology, guaranteeing quick and safe identity verification. Additionally, the paper includes IoT-enabled sensors and devices for real-time surveillance, which offer constant monitoring of critical areas to promptly detect unauthorised entrance or potential threats. Blockchain technology ensures transparency, immutability, and security

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14621435

against cyber attacks while protecting data transactions and records. Additionally, real-time system simulations and predictive maintenance are made possible by the use of digital twin technology, which promotes proactive decision-making and system optimisation. The document should be scalable, flexible enough to accommodate future advancements, and able to meet evolving military security requirements. By using cutting-edge facial recognition technology for robust access control, the system aims to increase security by making sure that only approved individuals may enter vital areas. The article makes use of IoT-enabled devices to provide real-time data collection and monitoring, which enables prompt identification of anomalies, potential hazards, and unauthorised activity. Blockchain technology protects data flows by offering immutability, transparency, and defence against online threats. Additionally, real-time simulations and predictive maintenance are made possible by digital twin technology, which offers crucial information for proactive decision-making. By offering a scalable, reliable, and extremely efficient solution to growing defence concerns, these technologies seek to completely transform defensive security systems. Figure 1 depicts the fundamental block chain architecture.

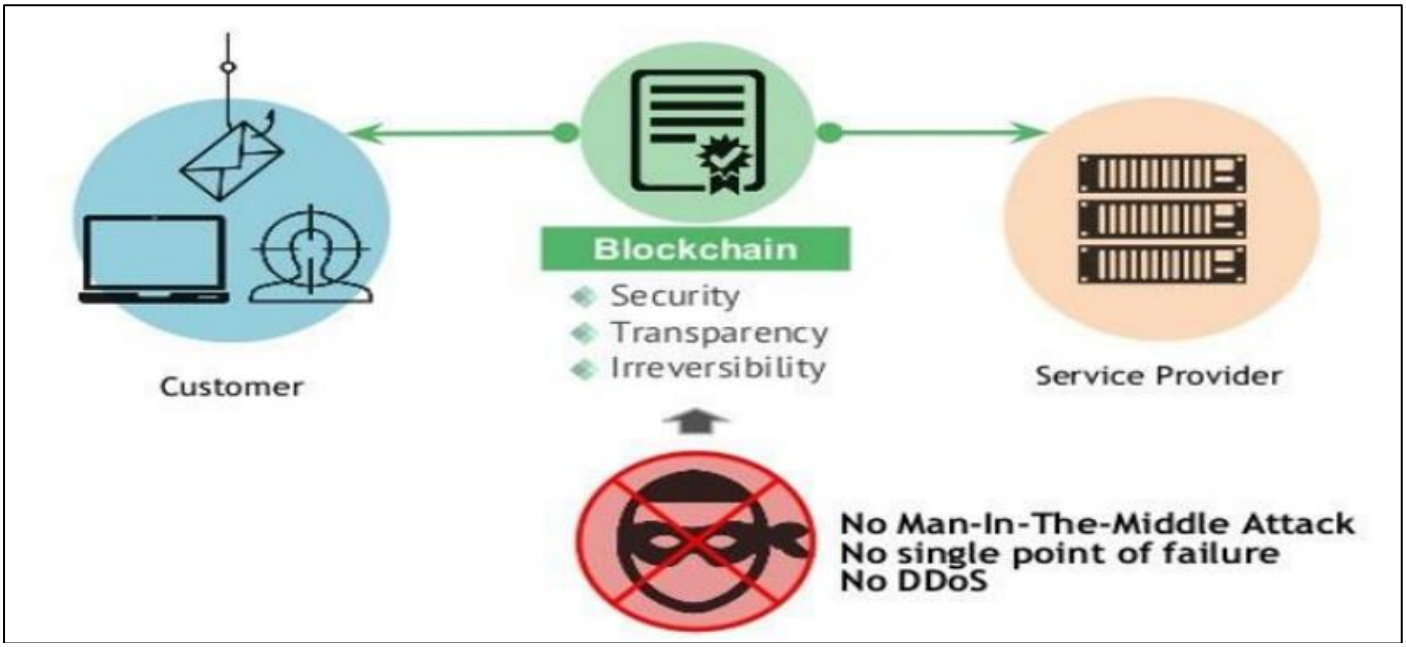

Fig 1 Block Chain Framework

II. RELATED WORK

P. Pătrașcu, et.al,…[1] Crucial services are among the many industries where emerging technologies are becoming a prominent topic. Thus, the use of such technologies in sensitive areas of national security presents a serious challenge, which is reinforced by the characteristics that distinguish emerging technologies, namely the imprecision of assessing technical maturity over time. Despite some uncertainty, emerging technologies need to be carefully considered from a national security perspective as both potential threats and real opportunities. In this article, I will assess the Internet of Things (IoT) as a new technology and its impact on national security from the viewpoints of the military sector and the defence of vital infrastructure. The advantages of contemporary technology are becoming more and more important to today's society. As a result, changing technologies have a big influence on people's lives as well as the functioning and security of the infrastructures that make it possible to deliver essential services and goods. Because of this, even in the most delicate areas of operation, it is now necessary to take use of emerging technology, which has significant implications for maintaining national security.

Jonathan ernestsirait, et.al,…[2] Because of characteristics that make daily chores easier, communication and information technology are becoming more and more popular every year. Organisations across a wide range of disciplines and industries have used information and communication technology in a variety of ways to increase productivity and profitability. Digital manufacturing is defined as the intensive use of a digital model to digitise the supply, production, and delivery activities of networked organisations. The military industry, which is controlled by manufacturing companies, is being disrupted by the existence of information and communication technologies in the 4.0 industrial era. Without a doubt, the demands of modern industrial enterprise differ greatly from those of the early Industrial Revolution. Resource conservation and process sustainability are given equal weight with quantity and quality in modern manufacturing. To stay competitive and prevent being overtaken by international rivals, the manufacturing sector must also adopt digitalisation, such as smart manufacturing or cloud computing, in the face of a global economy influenced by political pressure, shifting environmental conditions, technological breakthroughs, and fierce business rivalry. In addition to reducing unnecessary expenses and increasing operational profitability, digitalisation enables real-time monitoring and enhancement of product production, marketing, and after-sales activities.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14621435

Pradip kumarsharma, et.al,…[3] The use of connected smart devices has increased in military organisations in recent years. The full realisation of ubiquitous sensing, networking, and computation is known as the Internet of Battlefield Things (IoBT). Connectivity and cooperative decision-making over battlefield resources and combat gear are two of IoBT's unique characteristics. Conversely, edge computing gets beyond the drawbacks of conventional centrally planned network designs. Data collection and processing take place at or close to the application's source or device when computing and storage resources are positioned at the network's edge. By connecting wearable computing devices on the battlefield, edge computing enables military organisations to increase personnel safety and decision-making accuracy. The purpose of wearable computing in the military automation system is examined in this study. We offer a taxonomy of wearable computing in military automation systems and describe how each component relates to the others. We also describe the issues and challenges in cyber security and communication that come up when using the 5G network for defence automation. Additionally, in the context of 5G, we propose the design of the wearable wristwatch architecture as an example of healthcare transformation in defence automation.

Munish bhatia, et.al,…[4] Industry 4.0 is a result of the Internet of Things (IoT) being a major force behind innovation in smart environments including healthcare, logistics, and agriculture. The world's technical advancement is being directed towards more sophisticated research and discoveries thanks to the advancements brought about by this paradigm shift. By evaluating data at the network edge, fog computing, an extension of the cloud computing platform, promises to allow IoT technology to generate original solutions for challenging time-sensitive scenarios. The combination of cloud computing, fog, and IoT has demonstrated a number of service delivery applications in the food industry. The growing focus on food technology has led to the development of cutting-edge, futuristic technologies for offering profitable food-related services. Information and communication technology (ICT) has been transformed in a number of industries, including logistics, healthcare, and agriculture, by the Internet of Things (IoT) and the fog-cloud paradigm. This study proposes a novel idea for smart restaurants to use game theory to assess food quality, motivated by the enormous advantages of IoT technology. In particular, this study suggests a clever approach of evaluating restaurant meal quality. Real-time data is gathered by a variety of IoT devices in order to evaluate the quality of food. The cloud platform facilitates the transmission of the data to the fog nodes.

Safdar hussainjaved, et.al,…[5] Cyber-Physical Systems (CPSs), which are software components that function similarly to hardware to automate industrial processes, collect real-time data, and interface with devices and sensors via Human-Computer Interfaces (HCI), are made possible by the Industrial Internet of Things (I-IoT). This multifaceted technology aims to boost consistency, find opportunities for growth, and unlock untapped potential. Interoperability and coordination across various systems can be enhanced by integrating IoT sensors, data analytics, data storage and integration, and machine learning with CPSsThe system collects data from various sensors embedded in different equipment, continuously feeding it into system analytics. Machine learning (ML) algorithms process this data to improve and optimize the system's performance over time. Advanced Persistent Threat (APT) attacks aim to exploit Cyber-Physical Systems (CPSs) integrated with the Industrial Internet of Things (I-IoT) through rapid attack techniques. ML algorithms have shown promise in detecting APT attacks within autonomous systems and malware detection environments. However, detecting stealthy APT attacks within I-IoT-enabled CPSs and achieving real-time detection accuracy remain significant challenges. To overcome these issues, a novel solution is proposed that utilizes the Graph Attention Network (GAN), a multidimensional algorithm capable of capturing behavioral patterns and relevant information that earlier methods overlooked. This approach uses masked self-attention layers to address the limitations of traditional Deep Learning (DL) methods that primarily depend on convolutions.

Munish bhatia, et.al,…[6] Advancements in information and communication technology (ICT) have led to the adoption of innovative technologies across various industries, such as healthcare, transportation, agriculture, and logistics. The Internet of Things (IoT) plays a central role in these developments, driving automation and decentralized intelligence as essential tools for the future of industries. With the increasing ability to integrate ambient intelligence, IoT devices are connecting the physical and cyber worlds to automate data analysis and facilitate intelligent decision-making. Rooted in IoT, concepts like Smart Cities, Cyber-Physical Systems (CPS), and Industry 4.0 have emerged, contributing to global development. In addition, fog computing, as an extension of IoT, has arisen to address the growing demand for real-time service delivery. The healthcare sector is one of the leading fields transformed by IoT, particularly in the development of smart medical applications. This work proposes an efficient home-based urine-based diabetes (UbD) monitoring system. The system is designed with four layers to predict and monitor diabetes-related urinary infections. These layers include the Diabetic Data Acquisition (DDA) layer, Diabetic Data Classification (DDC) layer, Diabetic Mining and Extraction (DME) layer, and Diabetic Prediction and Decision Making (DPDM) layer. This structure enables individuals to regularly track their diabetes measures and perform predictive analysis, allowing for early intervention and proactive management of their condition.

Munish bhatia, et.al,…[7] Fog computing serves as an innovative framework for deploying wireless applications at the user level. By enhancing wireless technology with fog computing, it has made possible several applications that were previously limited by technological constraints. However, a key challenge remains in efficiently scheduling tasks across geographically dispersed fog computing nodes. As wireless data continues to grow rapidly, distributing this data across various fog computing nodes is crucial for providing effective decision-making services. Managing the scheduling of diverse data and tasks across geographically

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14621435

distributed fog devices remains an ongoing challenge in achieving high levels of efficiency and performance. The Internet of Things (IoT) environments, consisting of millions of wireless devices, generate numerous tasks, each with its own specific resource needs. Traditional task allocation methods are inadequate for addressing time-sensitive resource demands. Scheduling at the fog computing level has recently become a significant area of research. In the current IoT era, the rapid generation of large volumes of cyber data, combined with a limited number of computing devices, has made efficient load balancing more complex than ever before. To achieve optimal scheduling, new techniques must be developed to deploy efficient, time-sensitive wireless applications..

Luning li, et.al,…[8] Heterogeneous IoT environments consist of millions of wireless devices, each creating tasks with unique resource needs. Traditional task allocation methods struggle to meet the time-sensitive demands of these tasks. Recently, scheduling tasks at the fog computing level has gained attention as an important research area. With the massive growth of cyber data and a limited number of computing devices in today's IoT world, efficiently allocating resources has become more difficult. To achieve optimal scheduling, improved methods are needed for deploying time-sensitive wireless applications.For instance, when associating a digital twin with an intelligent model, neglecting essential components like data collection and visualization can result in creating digital shadows or models instead of a true digital twin. This document explores the challenges of using digital twin technology, particularly in the aerospace sector, while also addressing its broader applications. It highlights the limitations that prevent effective use in safety-critical systems and offers a detailed look at the fundamental aspects of digital twins.The paper proposes three key aspects for future digital twins in aerospace, known as aero-Digital Twins (aero-DTs),

Xiaokangzhou, et.al,…[9] A-YONet is a deep neural network model designed to be lightweight, combining the strengths of YOLO and MTCNN to achieve efficient training and feature learning with minimal computing resources. It includes a dynamic anchor box adjustment mechanism, using a clustering scheme to modify bounding boxes, and a multi-level feature fusion process to improve training efficiency when dealing with multiple targets of different sizes. The model also features a multimarket identification technique, which improves accuracy when tracking many moving objects in real-time surveillance. Experiments were conducted using two datasets one public and one custom within an actual surveillance system. The results showed that A-YONet outperformed three baseline methods in real-time monitoring for smart IoT devices. Traditional Computer Vision Systems (CVS) are typically centralized, but with the rapid growth of surveillance devices and the increasing volume of high-quality IoT surveillance data, these centralized systems are facing greater challenges

Nobuyuki fukawa, et.al,…[10] This catalyst investigates the academic and managerial ramifications of the digital twin in terms of innovation management. This intriguing new technology has the potential to transform both upstream and downstream innovation activities by combining the physical and digital (Maddikunta et al., 2021). Furthermore, the digital twin connects with other Industry 4.0 technologies, such as 3D printing, big data, and artificial intelligence. Thus, the processes and products created by a digital twin are relevant to researchers and practitioners interested in these neighbouring technologies. At the moment, digital twin technology is still at an early stage of development and somewhat disconnected from a firm's overall innovation strategy. Our inquiry is forward-looking in character, serving as a catalyst for future innovation management research and practices. First, we look at the relationship between the digital twin and three associated technologies (3D printing, big data, and AI). Second, we develop a typology of four distinct digital twin types (monitoring, creating, enhancing, and replicating) and demonstrate their importance for innovation management. Third, we provide a series of case studies that demonstrate this typology and how the digital twin has been used in practice. Fourth, we create a set of future research paths in this area that includes a broad variety of innovation-related subjects, such as service innovation, co-creation, and product design.

III. EXISTING METHODOLOGIES

Traditional surveillance systems, such as CCTV cameras and motion sensors, have been widely used to monitor activities and record events for later analysis. While these systems provide valuable insights after incidents occur, they are limited in offering real-time situational awareness or proactively detecting potential threats during an event. However, with the rise of emerging technologies like IoT, the capabilities of surveillance systems have greatly improved. IoT enables real-time data collection, allowing a network of connected sensors and devices to continuously gather information. This connected system can quickly detect abnormalities and improve situational awareness across large areas, enabling security personnel to respond faster to potential threats.

IoT-enabled devices can include various data sources like temperature sensors, motion detectors, cameras, and environmental sensors, giving a more comprehensive view of the monitored area. Despite these advancements, IoT-based surveillance systems still face challenges, such as cybersecurity risks and scalability issues. Many IoT systems are vulnerable to cyberattacks because their centralized architecture allows attackers to compromise the entire system by targeting a single central hub. Additionally, as the number of connected devices grows, managing and processing the large volumes of data can overwhelm existing infrastructure, causing slow performance, data congestion, or even system failures. Figure 2 illustrates the current framework with hardware deployment.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14621435

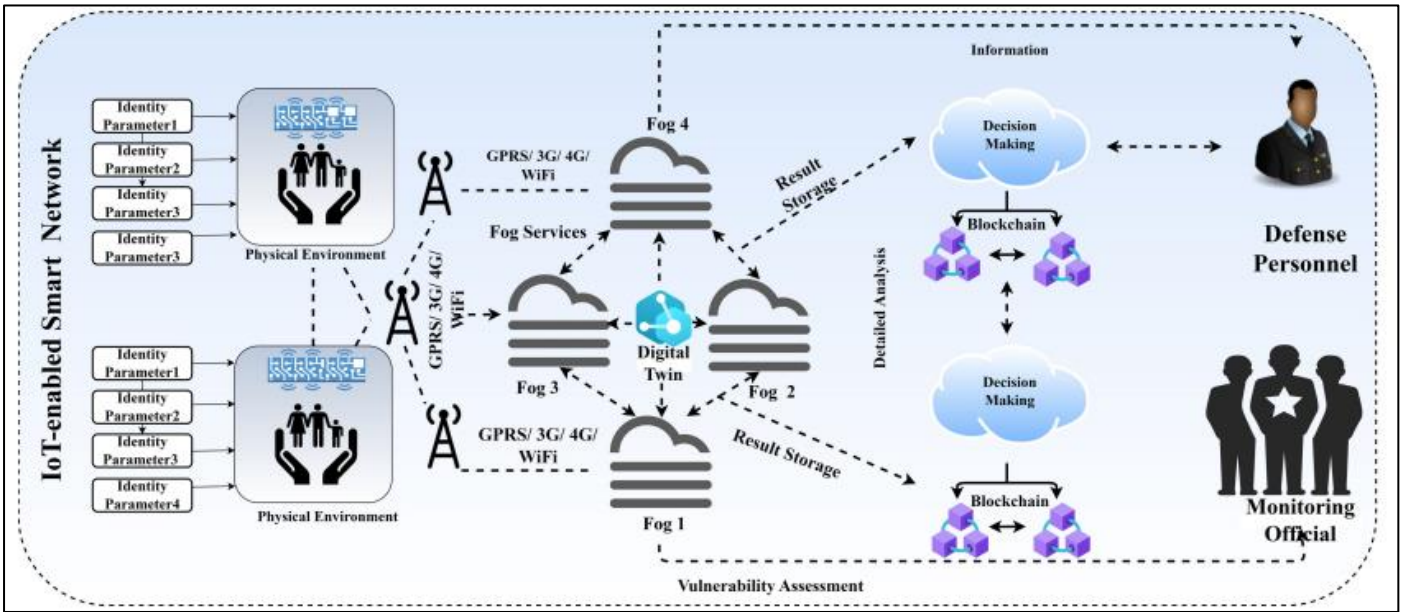

Fig 2 Existing Framework

IV. PROPOSED FRAMEWORK

The proposed integrated system aims to provide a comprehensive, real-time monitoring solution for military security. It includes secure data management, predictive analytics, and advanced access control, creating a robust and scalable defense infrastructure. The system uses cutting-edge technologies to build a flexible framework that meets current military needs. It continuously monitors vital assets and locations through IoT-enabled sensors and cameras, which collect and analyze real-time data. The data is securely transmitted and stored, offering fast insights and enabling quick responses to potential threats or anomalies. To securely manage critical defense data, the system uses Blockchain technology. A decentralized ledger ensures that data is stored in a secure, immutable format, protecting it from tampering. This is crucial for maintaining the integrity of information such as access logs, alarms, and surveillance footage. SHA-256 encryption within the blockchain adds an extra layer of security, defending against cyberattacks. Advanced access control based on facial recognition is a key feature of the system. It utilizes an improved Grassmann algorithm for identity verification, particularly in complex and dynamic environments. This method analyzes data in the Grassmannian space, ensuring high accuracy and reliability even in challenging conditions like low light, changing angles, and varying facial expressions. This innovative algorithm prevents unauthorized access to sensitive areas and offers a secure, contactless way to verify identity. Personnel are granted or denied access based on facial recognition, ensuring only authorized individuals can enter restricted zones. Figure 3 shows the proposed block diagram.

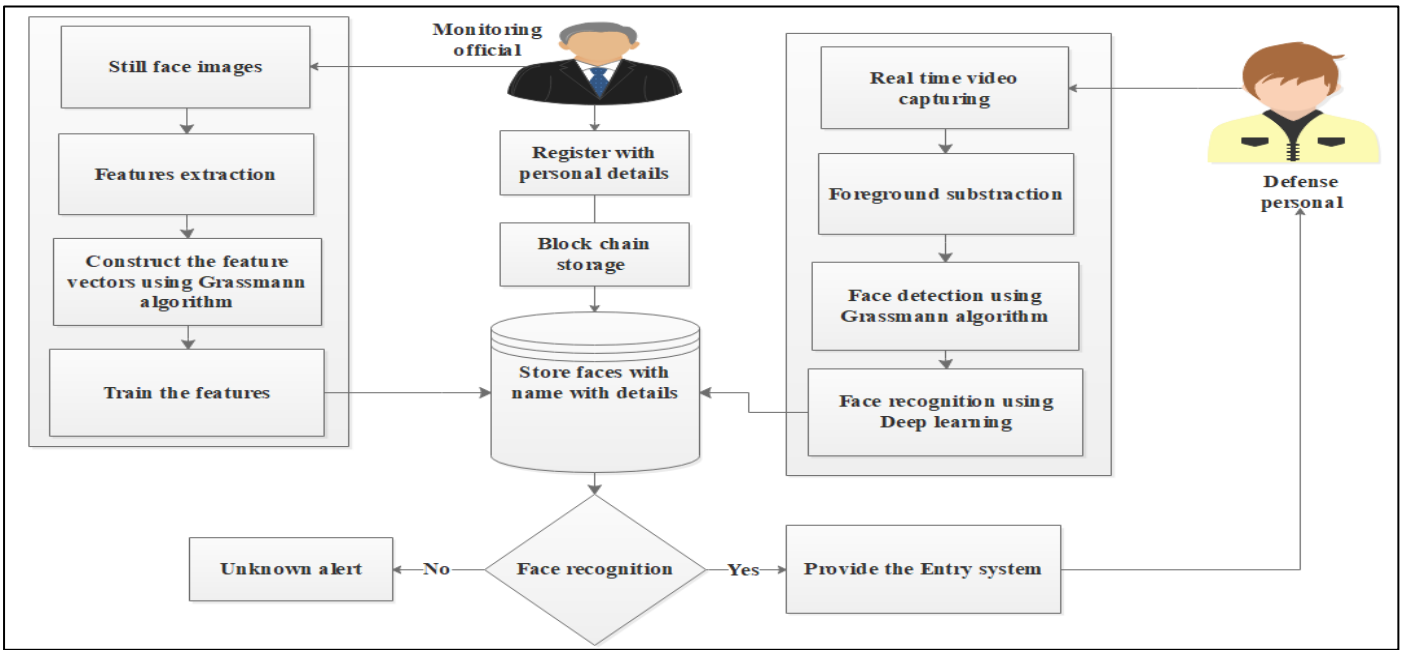

Fig 3 Proposed Framework

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14621435

➢ *Grassmann Algorithm*

Many image and video recognition systems use Grassmann manifolds to represent data. This study introduces a deep learning architecture that extends traditional Euclidean networks to Grassmann manifolds, enabling deep learning directly on these manifolds. The architecture includes several key components:

- Full rank mapping layers to convert input Grassmannian data into more useful forms.
- Orthogonal re-normalization layers to normalize the resulting matrices.
- Projection pooling layers to reduce model complexity in the Grassmannian context.
- Projection mapping layers to transform Grassmannian data into Euclidean forms for the final output layers.

The model is trained using stochastic gradient descent, with a matrix-based approach to backpropagation for updating the structured data. This novel network architecture is designed to process Grassmannian data directly, learning representations that improve visual tasks. It aims to fully learn Grassmannian data on their underlying Riemannian manifolds in an end-to-end learning framework.

Previous efforts often involve embedding the Grassmannian data into a Euclidean space, either by approximating it in the tangent space or using kernel functions in Hilbert spaces. These approaches allow traditional Euclidean techniques to be applied to the embedded data. For example, Grassmannian data can be embedded in a high-dimensional Hilbert space, where conventional methods like Fisher analysis are used. However, these methods are often limited to Mercer kernel-based classifiers and face increased computational complexity as the number of training samples grows. The Grassmann manifold, represented as G(m, D), refers to the set of m-dimensional subspaces in a D-dimensional space. It is a compact Riemannian manifold with m(D-m) dimensions.

An orthonormal matrix Y of size D by m can be used to correspond to an element of G(m, D), with Y = Im, where Im is the m by m identity matrix. For instance, Y may symbolize the m basis vectors of a set of R D photographs.

However, the matrices Y1 and Y2 are considered the same if and only if span(Y1) = span(Y2), where span(Y) signifies the subspace spanned by the column vectors of Y. In other words, if and only if Y1R1 = Y2R2 for some R1, R2 O, span(Y1) = span(Y2) (m). With this understanding, we will frequently use the notation Y to refer to its equivalence class span(Y), and Y1 = Y2 to refer to span(Y1) = span(Y2).

The length of the shortest geodesic linking two points on the Grassmann manifold is the Riemannian distance between two subspaces. However, utilising the principal angles to define the distances is a more perceptive and computationally well-organized method.

- Input: A set of P points on manifold

$\{X_i\}_{i=1}^{P} \in G(d, D)$

- Output: Karcher meanμK

- Set an initial estimate of Karcher mean $\mu_K = X_i$by randomly picking one point in $X_i\}_{i=1}^{P}$
- Compute the average tangent vector
- A $=\frac{1}{P}\sum_{i=1}^{P} \quad log_{\mu K}(X_i)$
- If $\|A\| < \varepsilon$ then return μK stop, else go to Step 4
- Move μK in average tangent direction $\mu K = exp_{\mu K}(\alpha A)$, where$\alpha > 0$ is a parameter of step size. Go to Step 2, until μK meets the termination conditions (reaching the max iterations, or other convergence conditions

V. EXPERIMENTAL RESULTS

Blockchain algorithms differ in terms of consensus, energy efficiency, scalability, security, and decentralisation, with each tailored to a distinct use case. Bitcoin uses Proof of Work (PoW), which requires miners to solve cryptographic problems to validate transactions, making it extremely secure but energy-intensive and sluggish, with limited scalability. Proof of Stake (PoS) chooses validators based on the amount of bitcoin they own and stake, giving better energy efficiency and faster transaction rates than PoW, but with modest decentralisation and susceptible to majority stake assaults. Delegated Proof of Stake (DPoS) enhances scalability by electing a limited number of delegates to validate transactions, making them quicker and more energy-efficient, but less decentralised and potentially vulnerable to delegate collusion. In contrast, Proof of Authority (PoA) relies on a few trusted authority nodes to confirm transactions, delivering very high scalability and efficiency but compromising decentralisation because it depends significantly on the honesty of validators. Table 1 shows the comparative analysis for proposed work.

Table 1 Comparison Details with Criteria

Criteria	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated PoS (DPoS)	Proof of Authority (PoA)
Consensus Mechanism	Mining solves cryptographic puzzles.	Stake-based selection of validators.	Voting among stakeholders to elect delegates.	Trusted validators (authority nodes).
Energy Efficiency	Low (high energy consumption).	High (energy-efficient).	High (energy-efficient).	High (energy-efficient).
Scalability	Limited (low TPS).	Moderate (higher than	High (optimized for	High (optimized for

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14621435

		PoW).	speed).	speed).
Security	Resilient but susceptible to 51% attacks.	Vulnerable if a majority stake is controlled.	Delegates could collude.	Dependent on authority honesty.
Decentralization	High (many miners).	Moderate (stakeholders).	Moderate (limited delegates).	Low (authority nodes).
Example Blockchains	Bitcoin, Ethereum (pre-Merge).	Ethereum (post-Merge).	EOS, TRON.	VeChain, BNB Chain.
Transaction Speed	Slow (~7 TPS for Bitcoin).	Faster than PoW.	Fast (up to 10,000 TPS).	Very fast (~10,000 TPS).

However, its reliance on a small number of nodes renders it less decentralised and therefore vulnerable to concerted assaults. Each algorithm proposes a trade-off between decentralisation, security, and performance, catering to diverse blockchain applications, including cryptocurrency and business networks.

VI. CONCLUSION

The Next-Generation Defence Security Framework combines Blockchain, IoT, Digital Twin Technology, and Advanced Face Recognition to provide a secure, scalable, and comprehensive solution for modern defence infrastructures. This system addresses real-time monitoring, secure data management, and predictive analytics to improve situational awareness and enable quick responses by defence personnel. Blockchain ensures that defence data is immutable and tamper-proof, protecting it from attackers. With decentralised ledgers and SHA-256 encryption, data integrity and confidentiality are maintained, while smart contracts automate and enforce security protocols. IoT enables continuous surveillance, early threat detection, and rapid response, enhancing the protection of critical assets and infrastructure. Digital Twin technology creates virtual replicas of physical assets, allowing real-time simulations and predictive maintenance. This helps identify and resolve potential issues before they become security risks, boosting operational efficiency. Advanced facial recognition, powered by the Grassmann algorithm, ensures precise identity verification and restricts access to authorized personnel, speeding up access control procedures. This integrated system is designed to be both secure and scalable, adapting to future technologies and evolving security needs. Its modular design allows for easy addition of new devices and sensors, ensuring the system remains effective in the face of increasingly complex threats.

REFERENCES

[1]. Pătraşcu, Petrişor. "Emerging technologies and National Security: The impact of IoT in critical infrastructures protection and defencesector." Land Forces Academy Review 26.4 (2021): 423-429.

[2]. Sirait, Jonathan, Hazen Alrasyid, and Nadia Aurora Soraya. "Strengthening The Defense Industry's Independence Through The Internet Of Things In The Manufacturing Sector: A Review." International Journal of Science, Technology & Management 4.2 (2023): 335-340.

[3]. Sharma, Pradip Kumar, et al. "Wearable computing for defence automation: Opportunities and challenges in 5G network." IEEE Access 8 (2020): 65993-66002.

[4]. Bhatia, Munish, and Ankush Manocha. "Cognitive framework of food quality assessment in IoT-inspired smart restaurants." IEEE Internet of Things Journal 9.9 (2020): 6350-6358.

[5]. Javed, Safdar Hussain, et al. "APT adversarial defence mechanism for industrial IoT enabled cyber-physical system." IEEE Access 11 (2023): 74000-74020.

[6]. Bhatia, Munish, et al. "Internet of things-inspired healthcare system for urine-based diabetes prediction." Artificial Intelligence in Medicine 107 (2020): 101913.

[7]. Bhatia, Munish, Sandeep K. Sood, and Simranpreet Kaur. "Quantumized approach of load scheduling in fog computing environment for IoT applications." Computing 102.5 (2020): 1097-1115.

[8]. Li, Luning, et al. "Digital twin in aerospace industry: A gentle introduction." IEEE Access 10 (2021): 9543-9562.

[9]. Zhou, Xiaokang, et al. "Deep-learning-enhanced multitarget detection for end–edge–cloud surveillance in smart IoT." IEEE Internet of Things Journal 8.16 (2021): 12588-12596.

[10]. Fukawa, Nobuyuki, and Aric Rindfleisch. "Enhancing innovation via the digital twin." Journal of Product Innovation Management 40.4 (2023): 391-406.