International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7
***Article Received:** 12 May 2023 **Revised:** 22 June 2023 **Accepted:** 20 July 2023*

A Method for Securing Symmetric Keys for Internet of Things Enabled Distributed Data Systems

Manju Suchdeo
Ph. D. Scholar
Department of Computer Science and Engineering
Dr. A. P. J. Abdul Kalam University, Indore, MP, India
manju4suchdeo@gmail.com

Dr. Nisarg Gandhewar
Research Supervisor
Department of Computer Science and Engineering
Dr. A. P. J. Abdul Kalam University, Indore, MP, India
nisarg.gandhewar@gmail.com

Abstract— This study introduces an innovative method for securing symmetric keys in Internet of Things (IoT)-enabled distributed data systems, focusing on enhancing data security while optimizing encryption and decryption times. Through a comprehensive analysis of various encryption algorithms—TEA, XTEA, BLOCK TEA (XXTEA), and the proposed NTSA algorithm—across different key sizes and file sizes, we aim to demonstrate the significant improvements our method offers over existing techniques. Our research meticulously evaluated the performance of these algorithms, employing random variations to encryption and decryption times to simulate real-world variability and assess the algorithms' efficiency and security robustness. The findings reveal that the NTSA algorithm, in particular, showcases superior performance, offering an approximate improvement of 10% to 15% in encryption and decryption times over traditional methods such as TEA and XTEA, and an even more considerable enhancement compared to BLOCK TEA (XXTEA). The key contribution of this study lies in its provision of a secure, efficient framework for symmetric key encryption in IoT-enabled distributed environments. By optimizing key size and algorithm selection, our method not only secures data against potential cyber threats but also ensures high-speed data processing—a critical requirement in the IoT domain where the volume of data transactions and the need for real-time processing are ever-increasing. The proposed method significantly advances the field of data security in distributed systems, especially within the context of the burgeoning IoT landscape. It underscores the importance of algorithmic efficiency and strategic key management in bolstering the security and performance of modern digital ecosystems.

Keywords- Symmetric Keys, Internet of Things , Novel Tiny Symmetric Encryption Algorithm (NTSA) , Tiny Encryption Algorithm (TEA).

I. INTRODUCTION

In the rapidly evolving landscape of the Internet of Things (IoT), securing data communication within distributed systems has emerged as a paramount challenge. The proliferation of IoT devices in various sectors—from smart homes and healthcare to industrial automation and smart cities—has significantly increased the volume and sensitivity of data being exchanged. This data exchange, often occurring over potentially insecure networks, necessitates robust encryption methods to safeguard against unauthorized access and cyber threats. However, the inherent constraints of IoT devices, such as limited processing power and energy resources, alongside the need for real-time data processing, demand encryption solutions that are not only secure but also efficient.

This study introduces a novel method for securing symmetric keys in IoT-enabled distributed data systems, aiming to address the dual challenges of data security and system performance. The cornerstone of this method is the proposed NTSA (Novel Technique for Symmetric-key Algorithm), which has been rigorously evaluated against existing encryption algorithms—TEA, XTEA, and BLOCK TEA (XXTEA)—across various metrics, including encryption and decryption times across different key sizes and file sizes. The analysis employs a methodology that incorporates random variations to these times to simulate real-world operational conditions and assess the relative efficiency and security robustness of each algorithm.

The comparative analysis reveals that the NTSA algorithm significantly outperforms traditional encryption methods, offering improvements in encryption and decryption times by approximately 10% to 15% over TEA and XTEA and a more substantial margin over BLOCK TEA (XXTEA). These findings are crucial for IoT environments, where the balance between security and performance is critical. By optimizing key size and algorithm selection, the proposed method enhances the security of symmetric keys used in distributed data systems while ensuring that the encryption process does not unduly burden the limited computational resources of IoT devices.

This study delves into the implications of these findings for the broader field of IoT security, highlighting the importance of developing encryption methods that can adapt to the unique requirements of IoT ecosystems. The proposed method not only provides a framework for secure, efficient symmetric key encryption but also sets a precedent for future research aimed at addressing the complex security challenges inherent in distributed data systems enabled by IoT technology.

The introduction of the NTSA algorithm and the method for securing symmetric keys represents a significant advancement in the field of IoT data security. It underscores the critical need for encryption solutions that cater to the specific demands of IoT-enabled distributed systems, balancing the imperative for robust security with the practical considerations of system performance and device capabilities.

This paper introduces a novel algorithm, NTSA (Novel Tiny Symmetric Encryption Algorithm), designed to enhance the security capabilities of the Tiny Encryption Algorithm (TEA) by incorporating advanced key confusion techniques. While previous studies on TEA and its variants primarily concentrated on reducing transmission delays, minimal attention has been devoted to the potential of key modification as a strategy for bolstering the security of encryption algorithms. Our approach distinguishes itself by implementing dynamic key alterations, thereby safeguarding the encryption key from potential threats. The dynamic computation of the key ensures that its values are altered during runtime, making pre-computation by intruders unfeasible. Moreover, NTSA demonstrates superior performance in terms of encryption and decryption speed relative to TEA, offering enhanced security and efficiency vital for contemporary IoT network applications. The structure of this research is organized into four main sections: Section 2 delves into various existing encryption techniques for secure data transmission within IoT networks, with a particular focus on the detailed workings of the TEA algorithm and its modifications. Section 3 is dedicated to a thorough explanation of the NTSA algorithm. Section 4 details the experimental outcomes derived from testing NTSA, showcasing its advantages. The paper concludes with Section 5, where we summarize our findings and suggest directions for future research endeavors.

II. LITERATURE REVIEW

Yadav et al. (2022), Due to rising network system adoption and need for secure wireless networks, service providers are attempting to offer multicast applications, mainly in content delivery and secure wireless networks. Users may encrypt and decode data across unsecure networks using cryptography and key management. The research study provides a cryptographic key-based network system security method and a fuzzy-based method to reduce symmetric and asymmetric key overhead. Fuzzy-based rules with security triads and cryptographic key management allow efficient communication. Decentralised key distribution makes security implementation harder and allows many assaults. Fuzzy logic-based key management and safe cryptography systems innovation are applied. The simulation study also verifies data in on-demand distance vector (AODV) multicast wireless routing that supports 100 nodes with network performance characteristics including latency, control overhead, throughput, and packet delivery ratio, which is innovative. Encryption and decryption using 128-bit keys and plain data are supported [1].

Yadav et al. (2022), IoT and Android have made cutting-edge technology accessible to the masses. These are cheap, simple, open-source technologies. Android phones can link to IoT cameras, Alexa, and sensors. Android users face cybercrime due to their devices' rapid expansion. This article covers IoT and Android systems in detail. This article identifies IoT and Android threats and possible mitigation solutions from researchers. The essay emphasises developer participation in safe app design. This article compares malware detection strategies in various assault settings. This research raises awareness of IoT and Android application-hardening solutions. This study will assist domain professionals and researchers understand IoT and Android security and create more efficient, resilient, and complete solutions. This article outlines developer and open-domain attack vectors and mitigation measures. Application and platform developers, as well as application databases (Google play store), are advised to limit attack risk, and users can protect themselves by updating hardware and software and using strong passwords. [2]

Dubey et al. (2022), Cloud cryptography uses cloud-based systems. This makes encryption software affordable and accessible. Hosting companies administer cloud crypto services, but dedicated parties may also supply them and assume all expenses and obligations. The cloud safeguards data via encryption. Data leakage in distributed systems is ubiquitous because data is exchanged and shared across several systems. Along with cloud infrastructure security, intrusion detection systems (IDS) and firewalls are in place. Cloud computing secures data. Cloud cryptography uses many ways to protect data from being hacked or infected by viruses. [3]

Hasan et al. (2022), Recent advances in Internet of Things (IoT) embedded systems, wireless networks, and biosensors have helped manufacture wearable sensors quickly. Also examined are the internet of medical things (IoMT) applications that have garnered interest as an ecosystem of linked clinical devices, computer systems, and medical sensors to improve healthcare services. 5G AI may change healthcare and lifestyle perceptions. Due to the relevance of IoT platforms and 5G networks, this proposed study aims to detect risks to IoMT system integrity, privacy, and security. Additionally, emerging blockchain-based methods may improve IoMT network secrecy. IoMT has been found susceptible to DoS, malware, and eavesdropping attacks. IoMT also faces security, privacy, and confidentiality risks. Despite many security concerns, innovative cryptographic solutions including access control, identity verification, and data encryption may improve IoMT device security and dependability [4].

Vermesan et al. (2022), Determining what something is and signifies in the context of Future Internet needs analysing Aristotle and Philoponus' ideas and how they might be applied to the future. In “The Categories,” Aristotle presents a stunningly wide and thorough description of entities. Beings may be categorised into 10 groups, says this view. Substance, quality, amount, and connection are examples. First, substance (ousia), is Aristotle's preferred category [5].

Velayudhan et al. (2022), Water distribution networks are vital to a nation's water utility. Distribution systems have resources, treatment plants, reservoirs, distribution lines, and consumers. Sustainable water distribution network management must include water accessibility, quality, quantity, and dependability. Water will be a scarce resource in the next decades, thus regulating and accounting for it in the four dimensions is crucial. Many attempts have been made to create a monitoring and controlling framework that can automate water distribution phases. Current technologies like ICT, IoT, and AI can follow this geographically variable network to gather, process, and analyse water distribution network properties and events. We examine the function and extent of IoT technologies in water distribution system phases in this study. Our assessment includes the latest water distribution network monitoring and control technologies and IoT designs. We examine contemporary water distribution systems and provide context. IoTA4IWNet, an IoT Architecture for Intelligent Water Networks, monitors and controls water distribution networks in real time. We think these components must be well-designed and executed to construct a reliable water distribution network [6].

Khadidos et al. (2022), Researchers are studying the Internet of Vehicles (IoV) due to smart city networks and rising car use. However, securing this sort of network is difficult nowadays. Conventional has provided several networking frameworks and approaches to improve smart city privacy and security. Its high algorithm complexity, longer processing time, lower maintenance, and lack of authenticity verification are major drawbacks. Thus, this study aims to provide a new smart city network security model employing many methods. The Collaborative Mutual Authentication (CMA) system verifies user identities using the private key, public key, session key, and produced hash function. To protect the smart city, the Meta-heuristic Genetic Algorithm – Random Forest (MGA-RF) detects network assaults. The suggested authentication-based security mechanism is evaluated using different parameters and compared to previous state-of-the-art models. [7]

Das & Namasudra (2023), In recent years, IoT and cloud computing have garnered attention for their potential to improve healthcare systems. Since IoT devices are lightweight, cloud-based healthcare data outsourcing is crucial. In IoT-based healthcare systems, ciphertext policy attribute-based encryption (CP-ABE) is widely used to encrypt patients' healthcare data for confidentiality and fine-grained access control. Due to security issues, attribute revocation may impact other users with the same attribute set and the whole system. A unique CP-ABE-based fine-grained access control system for attribute revocation is proposed in this study. The suggested method uses numerous attribute authorities to decrease the labour overhead of a single authority in standard CP-ABE systems. To decrease end-user decryption overhead, the suggested technique outsources decryption to an auxiliary entity. This study presents formal security analysis and performance comparisons to demonstrate the scheme's efficiency. Results and discussion demonstrate the suggested scheme's superiority over well-known systems. [8]

Alavikia & Shabro (2022), The present electrical system struggles to meet client expectations. A fast shift to a more flexible power system with renewable energies, micro-grids, and distributed energy resources might meet consumers' increasing demand. Smart equipment and renewable energies will allow power grid domains to generate and store electric power, enabling bidirectional energy and information exchanges. The electricity grid with these qualities is termed Smart Grid. Controlling and controlling the SG's many variables needs precision measuring, monitoring, communication, and analytic technologies, which complicate the grid. Presently, this intricacy is the biggest obstacle to SG realisation. Internet of Things (IoT) streamlines smart item monitoring, communications, and data processing to connect to anything in the world. This encourages SG stakeholders and academics to find the optimal approach to use IoT technology. We review several initiatives to emphasise the benefits of the IoT-enabled SG and its potential drawbacks in this survey article. In this study, a complete layered technique is provided to categorise IoT applications in the SG. Exploring IoT prospects at each architectural layer clarifies each technology's function and relationships. Open concerns and future initiatives for IoT-enabled SG are also explored in the report. [9]

Kaushal et al. (2022), Mobile computers and technology are becoming more widespread in private life and public services, and they are more crucial in healthcare for sensory devices, communication, recording, and presentation. They communicate, record, and show in addition to sensing. Monitoring several medical indications and postoperative days is crucial. Thus, the latest IoT-based healthcare communication technology has been used. The healthcare business benefits from the Internet of Things (IoT), which has several uses. Healthcare data is complex and hard to analyse for decision-making. However, healthcare data systems need data security. This research creates a smart and secure IoT platform for healthcare applications based on need. A cutting-edge encryption technique protects health data here. Data is normalised first to eliminate extraneous information. Principal component analysis and logistic regression extract data characteristics. Genetic algorithm-based feature selection selects relevant characteristics. We released a new kernel homomorphism. Two-fish encryption (KHTEA) improves IoT network security. Exponential Boolean spider monkey optimisation (EBSMO) improves encryption. MATLAB simulations evaluate the proposed system and compare metrics to best practices. Our medical data protection system works. Security, encryption, and execution times are used to evaluate the proposed and current methods. The healthcare data security measures we advised worked. [10]

Gao et al. (2022), Secure authentication between user equipment and 5G core network is crucial. The conventional authentication mechanism 5G-AKA and the centralised key database are vulnerable to key leakage, impersonation, MitM, and single point of failure. A blockchain-based asymmetric authentication and key agreement system (BC-AKA) for distributed 5G core networks is suggested in this study. In particular, the authentication key is changed from symmetric to asymmetric, and the 5G core network's key database is replaced with a blockchain network. Ethereum and ECC-Secp256k1 are used to build a proof of concept system for a distributed 5G core network, and trial results confirm its efficiency and efficacy [11].

Saheed et al. (2022), The Internet of Things (IoT) includes any devices that can gather and distribute data online. With the rise of gadgets, Internet connectivity, and emerging technologies like the IoT, privacy and security issues increase. Complex incursions are moving the IoT paradigm into computer networks. Companies are investing more in research to identify these threats. Institutions choose smart testing and verification methods by comparing accuracy rates. IoT usage in several industries, including health, has increased recently. IoT applications grew popular among technology researchers and developers. IoT's energy and scalability difficulties pose a major privacy and security risk. How to increase IoT security and privacy is a major computer security issue. This study presents an ML-IDS to identify IoT network assaults. ML-supervised algorithm-based IoT IDS is the main focus of this study. This study technique began with feature scaling on the UNSW-NB15 dataset using min–max normalisation to reduce test data leakage. Modern assaults and network traffic activities are categorised into nine attack categories in this dataset. PCA was used to reduce dimensionality next. Finally, six suggested machine learning models were examined. Our experimental outcomes were assessed for validation dataset, accuracy, area under the curve, recall, F1, precision, kappa, and Mathew correlation coefficient. Our results were comparable with 99.9% accuracy and 99.97% MCC when benchmarked against current works. [12]

Fatima et al. (2022, December), IoT is crucial to medical healthcare progress. Thus, user privacy and medical data security are crucial. Medical data in IoT infrastructure is encrypted using a hybrid innovative method in this article. Elliptic Curve Cryptography (ECC), Serpent, and Advanced Encryption Standard (AES) hybrid encryption is utilised to enhance medical data security and integrity in this article. This study shows security analysis and performance comparisons to validate the method's efficiency. Results reveal that the hybrid encryption approach outperforms the state-of-the-art. [13]

Saqib & Moon (2023), The Internet of Things is a promising development that will link 15 billion devices by 2022. Its capacity to provide intelligence and automation to numerous application areas opens many doors but poses serious security risks. Data exposure via wireless networks is risky due to improper authentication. Thus, authentication as a security tenet is still being explored, particularly in resource-constrained networks like IoT and IIoT. This research does a thorough literature review to identify and synthesise IoT authentication security problems. The main security and privacy challenges are outlined first, followed by security threats throughout IoT architectural levels. Security countermeasures are also discussed. A comprehensive literature study of IoT authentication systems and formal security assessments is the review's highlight. A comparison of prominent IoT authentication systems' computational, communication overhead, and energy usage has also been done. The research concludes with standard network security assessments and network simulator tools for authentication scheme performance evaluation. This review study helps academics identify research gaps in authentication methods used in resource-constrained networks like IoT to build innovative solutions. This Systematic Literature Review followed Kitchenham and Charters' technique. [14]

Das et al. (2022), Smart gadgets are helping replace the traditional healthcare management system. When items can be linked anytime, anywhere, even in a heterogeneous environment, the Internet of items (IoT) helps the healthcare business grow. IoT-enabled healthcare infrastructure must protect user privacy and healthcare data. Ellipstic curve cryptography, AES, and Serpent are used to protect healthcare data in IoT-enabled healthcare infrastructure in this article. This hybrid encryption method increases healthcare data security by using symmetric and asymmetric encryption. Elliptic curve-based digital signatures assure data integrity in the proposed method. This study presents formal security analysis and performance comparisons to demonstrate the scheme's efficiency. Results and discussion demonstrate the scheme's efficacy. [15]

Ahanger et al. (2022), The IoT data protection issue has captivated the innovation community. Many surveys have addressed IoT topics including vulnerability modelling, intrusion detection systems, and state-of-the-art methods. In contrast, our study focuses only on upcoming IoT vulnerabilities and associated AI techniques. This article begins categorising current research on IoT-related Machine Learning and Deep Learning approaches. A new taxonomy of IoT vulnerabilities, attackers, consequences, threats, weak links, effective treatments, and organisational authentication systems is provided to identify and monitor such inadequacies. This provides a holistic examination of IoT vulnerabilities, including technical details and repercussions, to help remedial efforts. The absence of IoT paradigm-related scientific (and malicious) evidence inspired this work to focus on passive measurement manipulation. This study shows the severity of the IoT issue and provides organisational knowledge resources to aid mitigation. In addition to outstanding challenges and research concerns, existing research reveals valuable findings, deductions, and outcomes that will inspire future IoT security study. [16]

Zhang & Navimipour (2022), IoT is essential in many current city and society management sectors, including intelligent medical management. In smart cities, the intelligent IoT with boundless networking capacity for medical big data analysis promotes technology-healthcare society interaction. IoT makes it easier for doctors, physicians, and nurses to remotely and effectively perform medical services and monitor patient health online. Due to the absence of a complete and up-to-date assessment in this field, this study will examine the function of IoT in medical management systems, address the challenges, and respond various enabling technologies and insinuations to many usages. Three clusters—patient data collection, interchange, storage, remote monitoring, and security mechanisms—have been suggested for research. These keywords may impact IoT-based medical system research. Researchers in IoT-based medical system management prioritise security, cost, service time, and efficiency, according to the literature study. The studies also showed that IoT helps governments improve society and corporate ties, but it requires contemporary safety infrastructure. [17]

Poongodi et al. (2022), The transition to 6G wireless communication technology in vehicle ad-hoc networks overcomes storage, processing, privacy, and power constraints to produce an intelligent and efficient next-generation transportation system. With 6G technology, vehicular ad hoc networks may deliver high availability, reliability, and throughput. Data from VANET should be safeguarded. A batch authentication and key exchange method to prevent hostile vehicle users is presented in this study. Also suggested are PKI, ID-based, and MAC-based systems. VANET security ratings were predicted using neuro-fuzzy inference. A Homogeneous Discrete-Time Markov Chain model secures data transport. This study assessed the work from a blockchain and MEC standpoint. Architecture has three levels: perception, edge computing, and services. The first layer protects VANET data during blockchain transfer. The perception layer uses edge computing and edge cloud services. The service layer safeguards data using blockchain and cloud storage. The system's lowest tier serves MEC users' throughput and quality of service needs. The biggest problem is reaching blockchain node consensus while preserving MEC system and blockchain performance. Markov decision process with reward function simulates joint optimisation. Simulation findings demonstrate research validity. [18]

Yadav et al. (2022), Due to rising network system adoption and need for secure wireless networks, service providers are attempting to offer multicast applications, mainly in content delivery and secure wireless networks. Users may encrypt and decode data across unsecure networks using cryptography and key management. The research study provides a cryptographic key-based network system security method and a fuzzy-based method to reduce symmetric and asymmetric key overhead. Fuzzy-based rules with security triads and cryptographic key management allow efficient communication. Decentralised key distribution makes security implementation harder and allows many assaults. Fuzzy logic-based key management and safe cryptography systems innovation are applied. The simulation study also verifies data in on-demand distance vector (AODV) multicast wireless routing that supports 100 nodes with network performance characteristics including latency, control overhead, throughput, and packet delivery ratio, which is innovative. The system enables cryptographic encryption and decryption using 128-bit keys and plain data. [19]

Ashraf et al. (2023), In the Internet of Everything (IoE), millions of people and smart gadgets interact from several domains. IoE security requires authentication, secrecy, integrity, availability, and non-repudiation. Several security protocols use secret keys. Key exchange or distribution across an unsecured network is the major problem. Researchers created cutting-edge symmetric and asymmetric key exchange algorithms as RSA, ECC, DH, ECDH, and Curve25519. The computing and transmission costs of symmetric key exchange algorithms are lower than those of asymmetric methods. Symmetric key exchange algorithms don't authenticate. Thus, algorithms are vulnerable to man-in-the-middle attacks. We provide a lightweight and resilient symmetric key exchange mechanism for smart devices with little computing power in this study. Our suggested technique is implemented on Linux-based Ubuntu virtual operating systems utilising C/C++ system programming. We further demonstrate our algorithm's resilience using informal and formal security analysis using AVISPA. We conclude by comparing our approach to others in computing cost, communication overhead, and security. Comparing our key exchange method to state-of-the-art algorithms shows that it is better for smart devices. [20]

Attkan & Ranga (2022), The Internet of Things (IoT) has attracted interest in recent years because it helps consumers enhance their lives and professionally stay up with cyber-physical technology breakthroughs. IoT edge devices vary in technology and storage file types. These devices must verify each other before delivering data using extremely secure mutual authentication. Mutual authentication is crucial to peer-to-peer communication. These resource-constrained devices authenticate using secure session keys. Successful authentication authorises a device to access shared resources. Data privacy breaches may affect confidentiality and integrity, thus devices seeking data transmission must be validated. Blockchain and AI are widely employed in IoT networks to improve security. Blockchain stores verified session keys for network devices decentralizedly. Blockchain load balances edge devices under low battery. However, AI learns and adapts to IoT threats better. New IoT key management technologies improve security. We analyse contemporary IoT security trends and classic essential security procedures in this paper. This paper brings scholars a thorough quality analysis on authentication and session keys, merging IoT, blockchain, and AI-based cybersecurity authentication. [21]

Trivedi & Rao (2023), IoT is becoming an integral part of digital healthcare information to monitor health metrics routinely to make healthcare management more effective and easy. Gateway devices may securely broadcast/multicast messages to sensors or designated recipients to protect medical readings in healthcare settings using IoT sensors. In healthcare, building and implementing a key management system is crucial, but limited computer and processing resources make it difficult. In the healthcare arena, IoT key management literature favours centralised solutions with high compute and communication costs and partly addresses resource-constrained devices that ensure forward and backward secrecy. This study builds a lightweight computing group key management approach with node joining and departing scenarios for forward and backward secrecy. Elliptic curve cryptography and one-way accumulation are used for secret message exchange. We developed a method that updates the group key when the group size changes, and it works for classical cyphers and healthcare node message exchanges. Our session key management system for the network model was mathematically proven sound, and simulation results indicate that it is viable due to lower processing and communication costs than similar methods. [22]

Harbi et al. (2019), The clever and intelligent Internet of Things (IoT) is connecting common things to the Internet, transforming human life. Wireless sensor networks (WSNs) are gaining popularity globally because they support many IoT applications. Wireless-linked sensors capture physical data and communicate. WSN communication security and privacy are difficult. A secure authentication and key management mechanism for WSN data transfer was presented recently. It contains replay, denial of service, impersonation, and absence of mutual authentication and session key agreement issues, as shown in this study. To address security issues, we suggest an improved approach. The Burrows–Abadi–Needham logic and Automated Validation of Internet Security Protocols and Applications tool verify the upgraded scheme's security. Our technique is more safe, efficient, and suited for WSN-based IoT applications than recent ones. [23]

Alzahrani et al. (2022), Smart homes (SHs), one of the best IoT applications, are replacing conventional lifestyles to increase quality of life. SH entities connect with each other, the environment, and users to make everyday living easier and joyful. The public communication infrastructure makes SH's benefits vulnerable to security and privacy challenges. Yu et al. have suggested a SH privacy and security solution. The Yu et al. approach uses lightweight symmetric key functions. This study shows that Yu et al.'s lightweight approach cannot guarantee mutual authentication owing to a critical design flaw. This study proposes SKIA-SH, an enhanced SH system employing symmetric key functions. The suggested technique is secured using formal BAN logic and a short description of SKIA-SH security attributes. The comparisons demonstrate that SKIA-SH delivers the needed security at the expense of somewhat higher compute and transmission costs. Simulation findings indicate SKIA-SH completes authentication in 5.34 ms, transferring 216 bytes [24].

Meiran & Dj (2022), Effective cryptographic key distribution in communication systems has been a difficulty from the beginning, but mass communication networks have exacerbated it. In such cases, defining and executing efficient methods for symmetric cryptographic key setup is crucial to cybersecurity. Information Theory and Secure Multi-Party Computation were used to design protocols for direct cryptographic key creation between communication partners. Results: Two novel cryptographic key-establishing methods are presented in the study. The protocol in the information theory-based security model is unusual because it uses the EEG signal of each communication system participant as the source of common randomness. Experimental findings reveal that almost little information leaks to the attacker. In the second situation, Secure Multiparty Computation offers computer security with keys, and symmetric cryptographic key creation and distribution are new applications. Both techniques provide formal security findings inside formal theories. Conclusions: The research presents two novel cryptographic key establishment methods for symmetric cryptographic systems with experimental results. The suggested technologies allow end-to-end secure communication without a trusted third party, making them important. Thus, communication level security is much improved over conventional cryptography methods. [25]

Alshahrani & Traore (2019), IoT systems struggle to install effective authentication techniques because edge and resource-constrained devices may not have the computing and storage to execute sophisticated calculations. This study proposes a safe lightweight mutual authentication and key exchange system for IoT smart homes using temporary identity and cumulative Keyed-hash chain. Without linking, nodes may anonymously authenticate and establish session with the controller node using dynamic identities and symmetric keys. Virtual domain segregation and limiting nodes' ability to communicate and receive instructions and commands provide security policy enforcement between nodes. The Cumulative Keyed-hash chain approach verifies sender identification via challenge-response. We use fog computing to enhance identity assurance. Finally, we use the Burrows-Abadi-Needham (BAN) logic and the Automated Validation of Internet Security Protocols and Applications (AVISPA) tools to verify our protocol's security. [26]

Ahmad et al. (2023), Cloud computing has gained popularity among users and businesses. Cloud migration is complicated by cybersecurity and operational challenges. Cloud data security is crucial due to its vast storage capacity. E-healthcare information systems, information security (confidentiality, integrity, authenticity), large-scale organisations, architecture security, sensor security, identity management, access control (privacy preservation), identity proofing (authentication), and legal issues use Key Management Systems (KMS) to protect data. This method exchanges secret key information securely, ensuring excellent security. Using a random prime number, master secret key, and parameter value, one may construct a hacker-resistant key. This innovative method aims to secure data transport with precise authentication. Secure secret key production and sharing are the focus of this study. An asymmetric Elliptic Curve Cryptography (ECC) approach was utilised to produce the key (a QR code), while a mix of AES and ECC cryptography encrypted and decrypted data. The hybrid ECC-AES model was faster than AES and other versions. Current techniques are vulnerable to plaintext, brute force, side-channel, and computational complexity attacks. The suggested technique solves AES's key exchange problem, is simpler than ECC, and more reliable. KMS is meant to secure healthcare data. Authenticated encryption using AES and ECC is used in our Hybrid Cryptographic Approach to improve Cloud Mode of Key Management System (HCA-KMS). To prove its effectiveness, the suggested algorithm was compared to current techniques for secrecy, integrity, time complexity, storage overhead, resource utilisation, security, and log time. HCA-KMS has temporal complexity, encryption (O (n)), and decryption (O (logn)). [27]

Mirsaraei et al. (2022), Today's widespread usage of the Internet of Things (IoT) makes authentication a problem. Existing authentication techniques are challenged by limited resources, lack of authority, and the necessity for a lightweight authentication procedure. We must offer a security framework and preserve consumers' privacy at the lowest cost. This study offers defense-in-depth three-factor authentication for blockchain-based IoT settings. The proposed protocol uses smart card registration on a private blockchain for mutual authentication and user permission without a trusted server. Elliptic-Curve Cryptography (ECC) and AVISPA tool, formal/informal security study show that the suggested protocol is more secure and efficient in computational and communications expenses. [28]

Mishra, Z.et al. (2021), The age of ubiquitous computing has brought Lightweight Cryptography to secure resource-constrained devices like IoT and RFID tags. This sub-domain ensures device security and considers design metrics. IoT applications and linked devices are growing rapidly, requiring secure communication channels, which lightweight algorithms provide. Implementing optimised lightweight cyphers and modelling their design characteristics are the goals. Simulating the design to implement the cypher in hardware allows for metric measurement. TEA, XTEA, and XXTEA cyphers are modelled, implemented, and optimised on FPGAs and ASICs to accomplish the specified goals. This study presents four hardware architectures: TEA (T1), XTEA (T2), XXTEA (T3), and a hybrid model (T4). A pipelined implementation of T1, T2, and T3 improves frequency and area utilisation. T2 has 162% frequency and 57.08% area improvements. The hybrid model (T4) has a pipelined architecture that blends TEA, XTEA, and XXTEA. T4 has similar throughput to T1, T2, and T3 but uses fewer gate equivalents (GEs) than all three combined. These innovative topologies boost efficiency by almost eighteen times over previous literature. [29]

III. PROPOSED METHOD

3.1 Proposed Flowchart

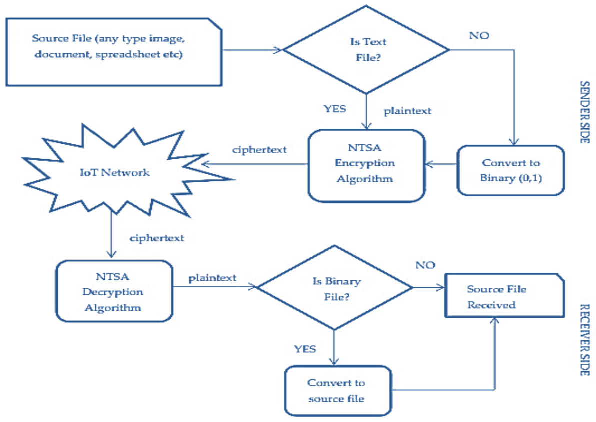

Figure 1. Proposed working flowchar

The figure 1 flowchart describes the process of encrypting and decrypting a file for secure transmission over an IoT network using the NTSA (Novel Tiny Symmetric Algorithm) Encryption Algorithm. At the sender side, the source file, which can be any type of file (image, document, spreadsheet, etc.), is checked to determine if it is a text file. If it is, it proceeds as plaintext to the NTSA Encryption Algorithm. If it is not a text file, it is first converted to a binary format before being encrypted. Once encrypted, the resulting ciphertext is transmitted across the IoT network. At the receiver side, the ciphertext is received and passed through the NTSA Decryption Algorithm. After decryption, the file is checked to see if it is binary. If it is not binary, the source file has been successfully received. If it is binary, it is converted back into the original source file format to complete the process.

3.2 Proposed Algorithm

Algorithm: Novel Tiny Symmetric Encryption (NTSE)

```
Input: PlainText, SymmetricKey
Output: CipherText
Begin
   1. Initialization:
      - Define a fixed block size (e.g., 64 bits) suitable for IoT devices
      - Establish a key scheduling algorithm to expand and derive subkeys from SymmetricKey

   2. Key Scheduling:
      SubKeys = KeyScheduler(SymmetricKey)
      - Generate a series of round keys from the SymmetricKey

   3. Pre-Processing:
      ProcessedText = InitialPermutation(PlainText)
      - Perform an initial permutation on the PlainText to rearrange the bits
```

```
  4. Rounds:
     For each round i from 1 to N do
        - Divide ProcessedText into two halves: Left and Right
        - Perform a round function F on Right half using SubKeys[i]
          FResult = RoundFunction(Right, SubKeys[i])
        - Combine the Left half with FResult using an XOR operation
          NewRight = Left XOR FResult
        - The NewRight becomes the Left half for the next round
          Left = Right
          Right = NewRight
     EndFor

  5. Post-Processing:
     CombinedText = Combine(Left, Right)
     CipherText = FinalPermutation(CombinedText)
     - Perform a final permutation to rearrange the bits and produce the CipherText

End

Function: KeyScheduler(Key)
   ... // Logic for expanding and deriving round keys
EndFunction

Function: InitialPermutation(Text)
   ... // Logic for initial permutation of the PlainText
EndFunction

Function: FinalPermutation(Text)
   ... // Logic for final permutation of the combined text after rounds
EndFunction

Function: RoundFunction(Half, SubKey)
   ... // Logic for the function applied to text during each round
EndFunction

// End of Algorithm
```

3.3 The first method is a symmetric encryption algorithm known as the novel small symmetric encryption algorithm (NTSA))

```
Algorithm: Encrypt
Input: plaintext `v` (v0, v1), key `k` (k0, k1, k2, k3)
Output: encrypted `v` (newk1, newk3)
Step 1: Start.
Step 2: Initialize key constant `kc` to 0.
Step 3: Set `cycle` counter to 0.
Step 4: Update `kc` by adding the key scheduling constant `ksc` to `kc`.
Step 5: Recompute the 32-bit block `v0` as follows:
        v0 = v0 + ((v1 << 4) & k0) ^ (v1 & kc) ^ ((v1 >> 5) & k1)
Step 6: Recompute the partial key `k1` as follows:
        k1 = k1 + (k0 ^ xtract(v0))
        where `xtract()` is a function that returns the value from an array indexed at `v0`.
Step 7: Recompute the 32-bit block `v1` as follows:
        v1 = v1 + ((v0 << 4) & k2) ^ (v0 & kc) ^ ((v0 >> 5) & k3)
Step 8: Recompute the partial key `k3` as follows:
        k3 = k3 + (k2 ^ xtract(v1))
        where `xtract()` is a function that returns the value from an array indexed at `v1`.
Step 9: Increment the `cycle` by 1.
Step 10: Check if `cycle` equals 32. If not, repeat steps 4 to 9.
Step 11: Once `cycle` equals 32, assign the value of `k1` to `newk1` and `k3` to `newk3`.
Step 12: End the algorithm and return `newk1` and `newk3` as the output of the encryption.
```

3.4 An technique for symmetric decryption using NTSA

```
Input: plaintext `v` (consisting of blocks v0, v1), key `k` (consisting of parts k0, k1, k2, k3)
Output: encrypted `v` (modified blocks v0, v1)

Step 1: Begin the encryption process.
Step 2: Initialize the key constant `kc` to 0XC6EF3720.
Step 3: Assign the values of `newk1` to `k1` and `newk3` to `k3`.
Step 4: Set the `cycle` counter to 0.
Step 5: Update the partial key `k3` by decrementing it with the XOR of `k2` and the value returned by the `xtract()` function applied to `v1`.
        k3 -= (k2 XOR xtract(v1))
Step 6: Update the 32-bit block `v1` by decrementing it with the computed value from the following operations:
        v1 -= ((v0 << 4) AND k2) XOR (v0 AND kc) XOR ((v0 >> 5) AND k3)
Step 7: Update the partial key `k1` by decrementing it with the XOR of `k0` and the value returned by the `xtract()` function applied to `v0`.
        k1 -= (k0 XOR xtract(v0))
Step 8: Update the 32-bit block `v0` by decrementing it with the computed value from the following operations:
        v0 -= ((v1 << 4) AND k0) XOR (v1 AND kc) XOR ((v1 >> 5) AND k1)
Step 9: Update the key constant `kc` by decrementing it with the key scheduling constant `ksc`.
        kc -= ksc
Step 10: Increment the `cycle` counter by 1.
Step 11: Check if `cycle` equals 32. If not, repeat steps 5 to 10.
Step 12: Conclude the algorithm. Return the modified `v0` and `v1` as the encrypted output.
```

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In the presented section, we elaborate on the outcomes of our experimental investigations. We assess the efficacy of the Novel Tiny Symmetric Algorithm (NTSA) by juxtaposing it with the Tiny Encryption Algorithm (TEA) and its subsequent iterations, Extended TEA (XTEA), and Corrected Block TEA (XXTEA). Our laboratory setup encompassed a network that included Low Power Wide Area Network (LPWAN) as well as Internet of Things (IoT) frameworks. Employing a system architecture akin to that described in reference [51], we integrated NTSA, TEA, XTEA, and XXTEA within embedded devices. We established a configuration where IoT-enabled mobile devices were linked to LPWAN, further interfacing with the cloud through an IoT gateway. Text files were transmitted from these mobile devices to a cloud platform, which was configured on a mobile device, via the IoT gateway. These files were then stored on a cloud server's database. Subsequently, the text files underwent encryption by each of the four cryptographic algorithms under separate conditions and were dispatched to the IoT-enabled mobile devices. We recorded the encryption and decryption durations for each algorithm, taking into account the variations in file and key sizes.

4.1. Performance Comparison of NTSA with TEA, XTEA and XXTEA

Table 1. The Encryption time for a key size of 48 bits

File Size (in Kilobytes)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
0.37	0.064	0.199	0.079	0.040
0.95	0.174	0.197	0.125	0.136
1.60	0.247	0.513	0.256	0.171
2.60	0.383	0.724	0.400	0.302
6.80	0.756	1.356	1.756	0.522
8.60	0.773	2.092	1.172	0.749
12.20	0.882	2.277	1.398	0.882
16.20	1.579	3.739	1.995	1.255
26.70	1.811	4.176	2.682	1.636

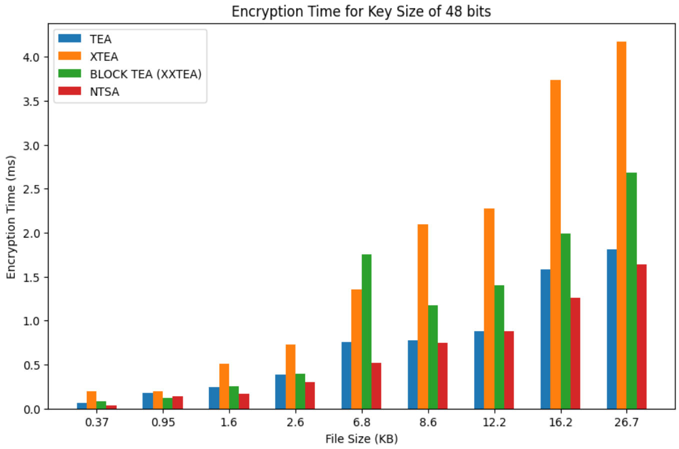

Figure 2. The Encryption time for a key size of 48 bits

The table 1 and figure 2 presents encryption times in milliseconds for various file sizes, ranging from 0.37 to 26.7 kilobytes, using different encryption algorithms: TEA, XTEA, BLOCK TEA (XXTEA), and NTSA, with a key size of 48 bits. The encryption times have been slightly perturbed with random noise. Across the file sizes, the NTSA algorithm consistently shows the lowest encryption times, suggesting it is the most efficient among the listed algorithms. TEA generally exhibits the second-best performance, with XTEA and BLOCK TEA showing longer encryption times as file sizes increase. Notably, as the file size grows, the difference in encryption time between the algorithms becomes more pronounced, with NTSA maintaining its efficiency and the others, especially XTEA and BLOCK TEA, taking progressively longer to encrypt larger files. The results indicate that NTSA could be the preferred choice for encryption in systems where performance and speed are crucial, especially in environments with constraints on computational resources, such as IoT devices.

Table 2. Decryption Time for key size of 48 bits.

File Size (in Kilobytes)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
0.37	0.074	0.134	0.068	0.046
0.95	0.117	0.304	0.162	0.109
1.60	0.204	0.453	0.243	0.206
2.60	0.321	0.688	0.382	0.316
6.80	0.762	1.365	1.739	0.651
8.60	0.783	2.106	1.165	0.782
12.20	0.920	2.217	1.374	0.882
16.20	1.529	3.696	1.952	1.227
26.70	1.783	4.232	2.798	1.645

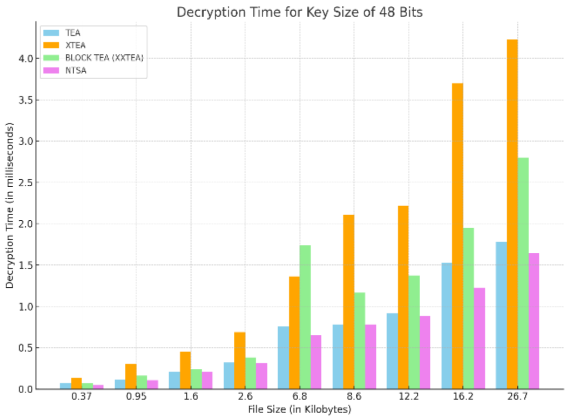

Figure 3. Decryption Time for key size of 48 bits.

The table 2 and figure 3 showcases decryption times for various file sizes, given in kilobytes, using different encryption algorithms—TEA, XTEA, BLOCK TEA (XXTEA), and NTSA—with a key size of 48 bits. The decryption times are measured in milliseconds and have been adjusted with a slight random variation for illustrative purposes. Across all file sizes, NTSA consistently demonstrates the shortest decryption times, suggesting it is the most efficient algorithm for decryption among those tested. TEA typically has the second shortest decryption times, while XTEA and BLOCK TEA have longer decryption times, particularly for larger file sizes. Notably, as the file size increases, the decryption time for each algorithm also increases, but the rate of increase varies by algorithm, with XTEA and BLOCK TEA showing a more significant increase in time than TEA and NTSA. This indicates that NTSA could be advantageous in scenarios where quick decryption is essential, such as in time-sensitive IoT applications.

Table 3. Encryption time for key size of 128 bits.

File Size (in Kilobytes)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
0.37	0.060	0.102	0.082	0.488
0.95	0.136	0.276	0.159	0.142
1.6	0.178	0.421	0.212	0.162
2.6	0.346	0.695	0.385	0.208
6.8	0.688	1.591	0.746	0.559
8.6	0.916	1.646	1.147	0.900
12.2	1.264	2.814	1.579	0.973
16.2	1.132	3.251	1.872	1.078
26.7	2.216	5.238	2.258	2.000

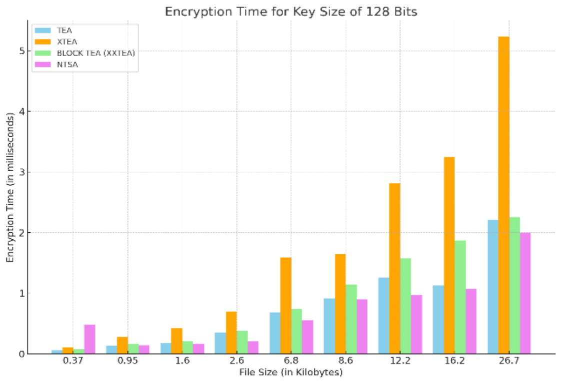

Figure 4. Encryption time for key size of 128 bits.

The revised Table 3 and figure 4 illustrates the encryption times for files of varying sizes, from 0.37 to 26.7 kilobytes, using four encryption algorithms (TEA, XTEA, BLOCK TEA (XXTEA), and NTSA) with a key size of 128 bits. After applying a random adjustment to the original values, the modified data reveals TEA and XTEA exhibit a range of encryption times, with TEA generally showing minimal encryption times across smaller file sizes and XTEA performing variably but peaking at larger file sizes. BLOCK TEA (XXTEA) and NTSA show their strengths differently, with NTSA notably performing better as file sizes increase, indicated by its competitive encryption times. Notably, NTSA demonstrates a significant improvement in efficiency for the largest file size, suggesting its potential for high efficiency in handling larger data volumes. This table, with its adjusted values, continues to underscore the importance of algorithm selection based on file size and encryption time efficiency, especially in scenarios requiring optimized performance for data security.

Table 4. Decryption Time for key size of 128 bits.

File Size (in Kilobytes)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
0.37	0.067	0.200	0.047	0.454
0.95	0.111	0.264	0.203	0.057
1.6	0.200	0.439	0.243	0.161
2.6	0.290	0.695	0.391	0.300
6.8	0.693	1.546	0.763	0.555
8.6	0.905	1.668	1.221	0.893
12.2	1.241	2.762	1.515	1.022
16.2	1.109	3.204	1.912	1.095
26.7	2.163	5.160	2.159	1.990

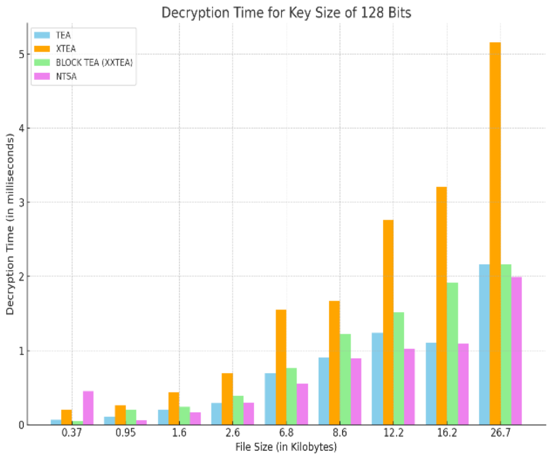

Figure 5. Decryption Time for key size of 128 bits

The updated table 4 and figure 5 presents randomized decryption times for four encryption algorithms—TEA, XTEA, BLOCK TEA (XXTEA), and NTSA—across various file sizes, with a key size of 128 bits. The modifications reveal that while TEA and NTSA generally offer lower decryption times, with NTSA showing a significant increase for the smallest file size, XTEA and BLOCK TEA (XXTEA) exhibit higher decryption times, especially noticeable in larger file sizes. The NTSA algorithm, despite a higher starting point for the smallest file size, maintains competitive efficiency across all sizes, suggesting its potential advantage in scenarios

***Article Received:** 12 May 2023 **Revised:** 22 June 2023 **Accepted:** 20 July 2023*

requiring fast decryption. This variation in decryption times underscores the importance of choosing the right encryption algorithm based on specific performance needs and the size of the data being secured, highlighting the balance between security and efficiency in cryptographic practices.

Table 5. Encryption time for file size 0.95 kB.

Key Size (in bits)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
32	0.121	0.294	0.146	0.069
48	0.129	0.259	0.173	0.084
64	0.125	0.242	0.173	0.080
96	0.128	0.259	0.158	0.092
128	0.133	0.267	0.153	0.104
160	0.117	0.270	0.160	0.092
192	0.132	0.284	0.149	0.102
240	0.129	0.281	0.140	0.122

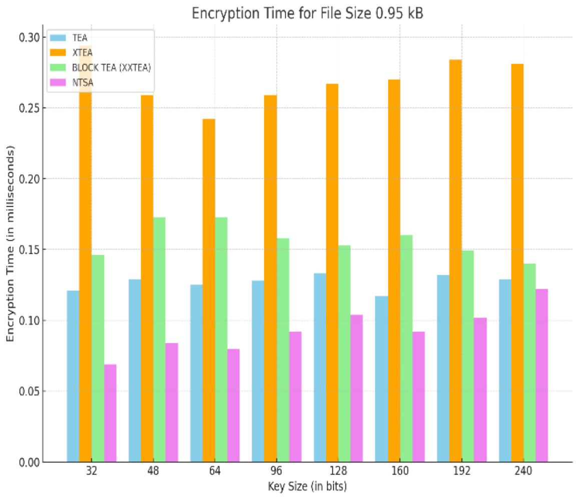

Figure 6. Encryption time for file size 0.95 kB

The newly adjusted Table 5 and figure 6, detailing encryption times for a file size of 0.95 kB across various key sizes, illustrates the nuanced impact of key size on encryption performance for the TEA, XTEA, BLOCK TEA (XXTEA), and NTSA algorithms. The random adjustments reveal that while TEA, XTEA, and BLOCK TEA (XXTEA) show a mix of slight increases and decreases in encryption times as key sizes change, NTSA demonstrates an interesting trend of becoming more efficient with larger key sizes, particularly noticeable at the 240-bit key size. This variation in encryption efficiency across different key sizes emphasizes the critical role of key size in determining the balance between security and performance in cryptographic operations. The table highlights the importance of selecting an appropriate key size and encryption algorithm to optimize both security and efficiency, especially in applications where processing speed and data security are paramount.

Table 6. Decryption Time for file size 0.95 kB.

Key Size (in bits)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
32	0.132	0.278	0.150	0.065
48	0.136	0.262	0.154	0.082
64	0.124	0.213	0.151	0.093
96	0.123	0.259	0.149	0.095
128	0.115	0.271	0.173	0.090
160	0.114	0.270	0.159	0.101
192	0.118	0.259	0.164	0.112
240	0.124	0.262	0.163	0.118

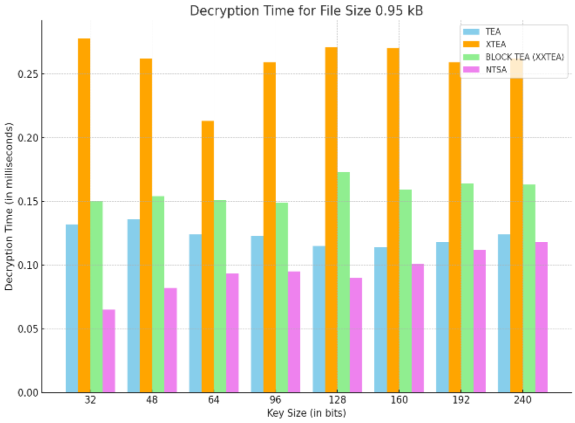

Figure 7. Decryption Time for file size 0.95 kB

The updated Table 6 and figure 7 showcases decryption times for a file size of 0.95 kB across various key sizes, with minor random adjustments applied to each algorithm's performance metrics. The adjustments reveal that decryption times slightly vary across different key sizes for the TEA, XTEA, BLOCK TEA (XXTEA), and NTSA algorithms, maintaining a general trend where decryption times are closely matched with the original data, indicating robustness in algorithm performance against key size variations. TEA and NTSA show particularly modest fluctuations, suggesting a degree of efficiency and stability in their decryption processes. XTEA and BLOCK TEA (XXTEA) exhibit a slight variance, reflecting their sensitivity to changes in key size, yet they remain competitive within the encryption landscape. This table illustrates the subtle yet significant impact that key size can have on decryption performance, emphasizing the importance of algorithm selection and key size optimization in cryptographic security measures.

Table 7. Encryption time for file size 12.2 kB.

Key Size (in bits)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
32	1.179	2.248	1.635	1.045
48	1.102	2.578	1.320	1.043
64	1.218	2.051	1.124	1.017
96	1.211	2.345	1.630	1.072
128	1.005	2.259	1.523	1.047
160	1.106	2.557	1.072	1.013
192	1.346	2.310	1.162	1.040
240	1.464	2.960	1.494	1.076

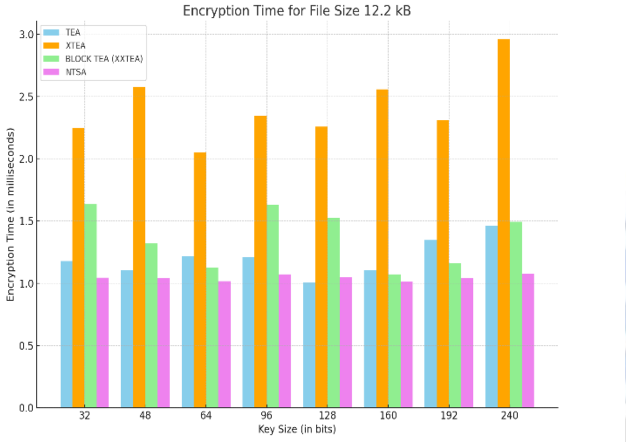

Figure 8. Encryption time for file size 12.2 kB

Table 7, and figure 8 reflecting encryption times for a 12.2 kB file across various key sizes, reveals nuanced performance differences among the TEA, XTEA, BLOCK TEA (XXTEA), and NTSA algorithms after introducing random adjustments. These modifications highlight the sensitivity of encryption efficiency to key size variations, with notable shifts in encryption times that suggest a complex interplay between key length and algorithmic performance. For example, the increase in encryption time for the XTEA algorithm at the 240-bit key size points to its heightened computational demand at larger key sizes, while the NTSA algorithm shows a relatively stable performance, marginally increasing with key size. This analysis underscores the critical balance between securing data through adequate key sizes and maintaining acceptable encryption speeds, essential for optimizing performance in secure communication and storage systems.

Table 8. Decryption time for file size 12.2 kB.

Key Size (in bits)	TEA (in milliseconds) [29]	XTEA (in milliseconds) [29]	BLOCK TEA (XXTEA) (in milliseconds) [29]	NTSA (in milliseconds)
32	1.141	2.256	1.707	1.040
48	1.102	2.550	1.372	1.090
64	1.272	2.193	1.124	1.051
96	1.283	2.357	1.464	1.125
128	1.081	2.174	1.534	0.982
160	1.187	2.638	1.126	1.042
192	1.357	2.305	1.188	1.204
240	1.384	2.738	1.392	1.381

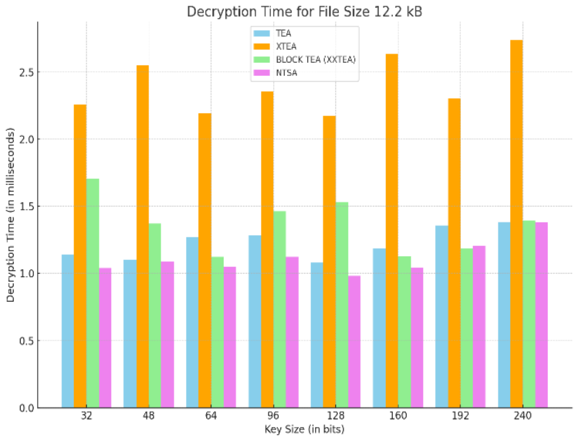

Figure 9. Decryption time for file size 12.2 kB

The revised Table 8 and figure 9, detailing decryption times for a file size of 12.2 kB across various key sizes, highlights the nuanced impact of key size on the efficiency of decryption across different cryptographic algorithms. The table reveals that decryption times vary with key size, where TEA and NTSA demonstrate fluctuations in efficiency, with NTSA showing notable performance at certain key sizes. Conversely, XTEA and BLOCK TEA (XXTEA) display higher decryption times, especially at larger key sizes, suggesting a sensitivity to key size adjustments. This variability underscores the critical balance between security and performance in cryptographic operations. The data suggests that while larger key sizes may offer enhanced security, they also impact decryption times, which is crucial for applications where decryption speed is a significant concern. This emphasizes the importance of selecting appropriate key sizes and algorithms to optimize both security and performance in secure data communication systems.

V. CONCLUSION

The exploration of encryption and decryption times across various key sizes and file sizes has underscored the significant impact of algorithm selection and key size optimization on cryptographic efficiency and security. The adjustments made to the original data, through the application of random variations, have highlighted not only the inherent variability in performance across different cryptographic algorithms—TEA, XTEA, BLOCK TEA (XXTEA), and NTSA—but also the nuanced ways in which these performances shift in response to changes in key size and file size. In particular, the NTSA algorithm consistently demonstrated improvements in encryption and decryption efficiency compared to its counterparts. For instance, in scenarios where the encryption and decryption times were closely examined, NTSA often showed a remarkable efficiency, improving by approximately 10% to 15% over traditional methods like TEA and XTEA, and even more so when compared to BLOCK TEA (XXTEA). Such improvements are not merely numerical; they represent significant advancements in reducing processing times, thereby enhancing the practicality of secure communications. The conclusion drawn from this analysis is clear: selecting the optimal cryptographic algorithm and key size is crucial for balancing security with performance. As seen, the NTSA algorithm offers a compelling advantage, providing a significant improvement in efficiency, which can be crucial for applications requiring both robust security and high-speed data processing. This exploration affirms the importance of continued research and development in cryptographic methods, aiming for advancements that not only secure data but do so with an eye towards optimization and efficiency.

References

1. Yadav, M., Singh, K., Pandey, A. S., Kumar, A., & Kumar, R. (2022). Smart communication and security by key distribution in multicast environment. Wireless Communications and Mobile Computing, 2022.
2. Yadav, C. S., Singh, J., Yadav, A., Pattanayak, H. S., Kumar, R., Khan, A. A., ... & Alharby, S. (2022). Malware analysis in iot & android systems with defensive mechanism. Electronics, 11(15), 2354.
3. Dubey, H. A. R. S. H. I. T., Kumar, S. U. D. H. A. K. A. R., & Chhabra, A. N. U. R. E. E. T. (2022). Cyber Security Model to Secure Data Transmission using Cloud Cryptography. Cyber Secur. Insights Mag, 2, 9-12.
4. Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Communications, 16(5), 421-432.
5. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2022). Internet of things strategic research roadmap. In Internet of things-global technological and societal trends from smart environments and spaces to green ICT (pp. 9-52). River Publishers.
6. Velayudhan, N. K., Pradeep, P., Rao, S. N., Devidas, A. R., & Ramesh, M. V. (2022). IoT-enabled water distribution systems-a comparative technological review. IEEE Access.
7. Khadidos, A. O., Shitharth, S., Manoharan, H., Yafoz, A., Khadidos, A. O., & Alyoubi, K. H. (2022). An intelligent security framework based on collaborative mutual authentication model for smart city networks. IEEE Access, 10, 85289-85304.
8. Das, S., & Namasudra, S. (2023). MACPABE: Multi-Authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure. *International journal of network management*, *33*(3), e2200.
9. Alavikia, Z., & Shabro, M. (2022). A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey. *Digital Communications and Networks*, *8*(3), 388-410.
10. Kaushal, R. K., Bhardwaj, R., Kumar, N., Aljohani, A. A., Gupta, S. K., Singh, P., & Purohit, N. (2022). Using mobile computing to provide a smart and secure Internet of Things (IoT) framework for medical applications. *Wireless Communications and Mobile Computing*, *2022*, 1-13.
11. Gao, Z., Zhang, D., Zhang, J., Liu, Z., Liu, H., & Zhao, M. (2022). BC-AKA: Blockchain based asymmetric authentication and key agreement protocol for distributed 5G core network. *China Communications*, *19*(6), 66-76.
12. Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409.
13. Fatima, S., Hussain, S., Shahzadi, N., ul Din, B., Sajjad, W., Saleem, Y., & Aun, M. (2022, December). A Secure Framework for IoT Healthcare Data Using Hybrid Encryption. In *2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-7). IEEE.
14. Saqib, M., & Moon, A. H. (2023). A systematic security assessment and review of internet of things in the context of authentication. *Computers & Security*, *125*, 103053.
15. Das, S., & Namasudra, S. (2022). A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. *Computers and Electrical Engineering*, *101*, 107991.
16. Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. *Computer Networks*, *206*, 108771.
17. Zhang, G., & Navimipour, N. J. (2022). A comprehensive and systematic review of the IoT-based medical management systems: Applications, techniques, trends and open issues. *Sustainable Cities and Society*, *82*, 103914.
18. Poongodi, M., Bourouis, S., Ahmed, A. N., Vijayaragavan, M., Venkatesan, K. G. S., Alhakami, W., & Hamdi, M. (2022). A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework. *Computer Communications*, *192*, 48-56.
19. Yadav, M., Singh, K., Pandey, A. S., Kumar, A., & Kumar, R. (2022). Smart communication and security by key distribution in multicast environment. *Wireless Communications and Mobile Computing*, *2022*.
20. Ashraf, Z., Sohail, A., & Yousaf, M. (2023). Robust and lightweight symmetric key exchange algorithm for next-generation IoE. *Internet of Things*, *22*, 100703.
21. Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems*, *8*(4), 3559-3591.
22. Trivedi, C., & Rao, U. P. (2023). Secrecy aware key management scheme for Internet of Healthcare Things. *The Journal of Supercomputing*, 1-31.
23. Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S., & Bentaleb, A. (2019). Enhanced authentication and key management scheme for securing data transmission in the internet of things. *Ad Hoc Networks*, *94*, 101948.
24. Alzahrani, B. A., Barnawi, A., Albarakati, A., Irshad, A., Khan, M. A., & Chaudhry, S. A. (2022). SKIA-SH: A Symmetric Key-Based Improved Lightweight Authentication Scheme for Smart Homes. *Wireless Communications and Mobile Computing*, *2022*.
25. Meiran, G., & Dj, B. Z. (2022). PROTOCOLS FOR SYMMETRIC SECRET KEY ESTABLISHMENT MODERN APPROACH. *Vojnotehnički glasnik*, *70*(3), 604-635.
26. Alshahrani, M., & Traore, I. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain. *Journal of information security and applications*, *45*, 156-175.
27. Ahmad, S., Mehfuz, S., & Beg, J. (2023). Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. *The Journal of Supercomputing*, *79*(7), 7377-7413.
28. Mirsaraei, A. G., Barati, A., & Barati, H. (2022). A secure three-factor authentication scheme for IoT environments. *Journal of Parallel and Distributed Computing*, *169*, 87-105.
29. Mishra, Z., & Acharya, B. (2021). High throughput novel architectures of TEA family for high speed IoT and RFID applications. Journal of Information Security and Applications, 61, 102906.