Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

An Enhanced Authentication Protocol (SAS) for Multi-server Architecture Integrating Mind Mapping based on Hashing Algorithm to Mitigate Digital Literacy threats in Higher Education: A Hybrid AI Assisted PBL

Syed Aale Ahmed
Department of Information Technology, Faculty of Computer Science & IT, Superior University, Lahore, 54000, Pakistan
Email: magharstar@gmail.com
Ali Hassan
Innova Networks, Lahore Pakistan Email: alihassan2590@gmail.com
Haseeb Ch
Innova Networks, Lahore Pakistan Email: haseebch552277@gmail.com
Nasir Ayub
Deputy Head of Engineering, Calrom Limited, M16EG, United Kingdom
Email: nasir.ayyub@hotmail.com
Umair Ghafoor
Deputy Head of Engineering, Calrom Limited, M16EG, United Kingdom
Email: umairghafoor@hotmail.com
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan Email: rizwan.naqvi@ieee.org
Hamayun Khan
Department of Computer Science,, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan Email: hamayun.khan@superior.edu.pk
Muhammad Zunnurain Hussain
Bahria University Lahore Campus, Email: zunnurain.bulc@bahria.edu.pk

ABSTRACT

The proliferation of distributed systems, cloud and the Internet of Things (IoT) has made the need for strong authentication mechanisms in multi-server systems all the more important. It is a very simple and inexpensive method of authentication; however, it is easily attacked with replay attacks, impersonation attacks, and offline password guessing attacks. Moreover, most of these schemes allow only partial anonymity to the users and use verification tables or complex cryptographic procedures to improve security but require a lot of computing power. Due to the rapid proliferation of Artificial Intelligence (AI) tools in higher education has created new opportunities and challenges for both learners and educators. This paper presents a comprehensive synthesis of four contemporary empirical studies examining the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

intersection of AI, Project-Based Learning (PBL/PjBL), mind mapping, digital literacy, and collaborative skills development. Drawing on co-design methodologies, inclusive education frameworks, and experimental research designs, the paper critically analyses how students interact with AI in project contexts, how AI-assisted mind mapping enhances creative thinking and digital competencies, and how collaboration skills develop when AI tools are integrated into structured learning environments. Findings indicate that AI-enhanced PBL consistently improves multiple learner outcomes, and that students with neurodevelopmental disorders demonstrate disproportionately strong gains. Implications for curriculum design, assessment, and future research are discussed. These restrictions shed light on the need for a lightweight, secure and scalable authentication solution. This research aims to design an authentication scheme that is simple and secure for multi-server systems, using one-way hash functions. The architecture of the protocol is based on multiple entities: Users, a registration center, and multiple service servers, through which a user can access a variety of services without having to register again. The protocol uses dynamic identity (DID) generation and random nonces, which ensures privacy and protects users from being traced across sessions. In addition, there is no need to use a verification table, which means that the risk of leakage of such credentials and the attacks by servers are greatly reduced. The proposed protocol offers user/server mutual authentication, secure key establishment and repel any replay attack by the nonces based communication. It also provides forward secrecy, creating unique session keys for each session of communication. The protocol is resource-friendly, as its computation and communication are both very light and suitable for resource-limited systems like the Internet of Things, mobile systems, cloud-based applications and the like. The simulations show that the proposed protocol is efficient in terms of computation and secure with high level of security. It solved the most important problems of the current multiple server authentication systems and established a practical, scalable and efficient solution for the current distributed computing environment.

Introduction

Digital technologies, cloud computing and distributed network systems have transformed computing environments almost beyond recognition. The users today use several online services like ecommerce platforms, cloud storage, banking system and Internet of Things (IoT) applications that all need secure authentication system [1, 2]. Authentication helps to ensure that users cannot access the system or the sensitive data they contain without permission. Of all authentication options, password based authentication is the most common due to its simplicity, low implementations costs and ease of use [3, 4]. While some more sophisticated methods have become available - biometrics and multi-factor authentication - the use of passwords is still widespread, particularly in resource-limited situations. Traditional password authentication systems have been built primarily to support single server applications and users have only one service provider with which they interact. Online service's growth, however, has introduced its own problems, though: users have to keep track of their various usernames and passwords [5]. This can lead to inadequate password habits like

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

reusing passwords and selecting weak passwords, creating security hazards for unauthorized entry and password stealing. Furthermore, a single-server authentication method does not work in today's distributed environments where users require access to several services without any re-authentication [6, 7].

$$T_{total} = \Delta T_{proc} + \Delta T_{det} + \Delta T_{exec} \quad \textbf{Eq (1)}$$

Multi-server protocols have been developed to solve the problems outlined above. These protocols enable registration with a trusted authority once, and access to multiple servers with security. This makes it more user friendly, lowers administration expenses and allows for centrally managed authentication. Because of the increased level of complexity of communications and the susceptibility to a variety of attacks such as replay, man-in-the-middle, impersonation etc, design of secure and efficient multi-server authentication system is still problematic [8, 9]. One of the main problems of many of the traditional authentication schemes is that they use verification tables on servers. These tables are a source for sensitive credential data and are a good target for attackers. They could allow offline password guessing attacks and impersonation if compromised. To overcome this problem, several table-less authentication schemes have been proposed [10, 11].
Where

ΔT_{proc} Shows the data processing time for features extraction and PCA reduction

$$\Delta T_{proc} = T_{PCA\_transform} \quad \textbf{Eq (2)}$$

Many of these solutions come with a high computational cost though, or provide only partial security guarantees. There is another important concern lack of users anonymity and privacy protection [12, 13]. Numerous authentication protocols send out the identity of the user in the clear or as a fixed value, which can enable an attacker to follow a user's activity. To enhance privacy, dynamic-based authentication schemes have been designed that mask and often change the identities of users [14, 15]. All of these schemes improve anonymity, but many have security flaws. Another factor that is important is computational efficiency. Today, there are public-key cryptography methods like RSA and elliptic curve cryptography (ECC) that are used in many current authentication protocols [16, 17]. While secure, they are costly and not a suitable option for lightweight devices, like IoT systems. Therefore, the concept of hash-based authentication protocol which is basically a one-way hash function has gained interest these days more and more because it is being used for good security with less computation overhead [18, 19]. The motivation of this study is that multi-server system requires secure, lightweight and efficient authentication protocol. Current protocols do not usually support all the required security properties at once: mutual authentication among parties, anonymity of users, cryptographic forward secrecy, protection against common cryptographic attacks and low computational complexity [20, 21]. To overcome these problems, the present research introduces a Simple and Secure (SAS) Password Authentication Protocol utilizing hash algorithm. The proposed protocol is designed to remove verification tables, offer dynamic identity protection, ensure mutual authentication, resist to popular attacks and have low computation overhead. This study is important because it helps in securing

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

distributed systems, like cloud systems, IoT and e-commerce [22, 23]. The following protocol provides stronger security, greater level of privacy, decreased storage and simple multi-server access as a result of the lightweight hash-based cryptographic mechanisms. The research study is conceptual so it is not created, however it is imperative for filling up an important research area by offering a balanced system that integrates security, e-commerce and user experience [24]. The integration of Artificial Intelligence (AI) into higher education represents one of the most transformative pedagogical shifts of the 21st century. As AI tools grow increasingly accessible and capable, their adoption by university students has expanded from a novelty to a near-ubiquitous reality. Students now routinely deploy AI systems to support learning tasks ranging from code debugging and documentation to creative ideation, research analysis, and collaborative project work [25, 26].

ΔT_{det} Shows the detection latency of AI inference time.

$$\Delta T_{det} = T_{LSTM\_inference} + T_{RF\_classification} \qquad \textbf{Eq (3)}$$

ΔT_{exec} Shows the execution latency time for the SDN controller to push flow rules.

This shift compels educators, curriculum designers, and researchers to grapple with fundamental questions about the nature of learning, assessment authenticity, and skill development in an AI-augmented world. Project-Based Learning (PBL), a pedagogy grounded in constructivist theory, has long been recognised as an effective method for developing higher-order thinking, collaboration, and authentic problem-solving [27, 28]. By engaging students in extended, real-world projects that produce tangible artefacts, PBL naturally accommodates technology use, including AI tools. Yet the specific ways in which AI intersects with PBL processes, assessment validity, creative development, digital literacy, and peer collaboration remain incompletely understood [29, 30].

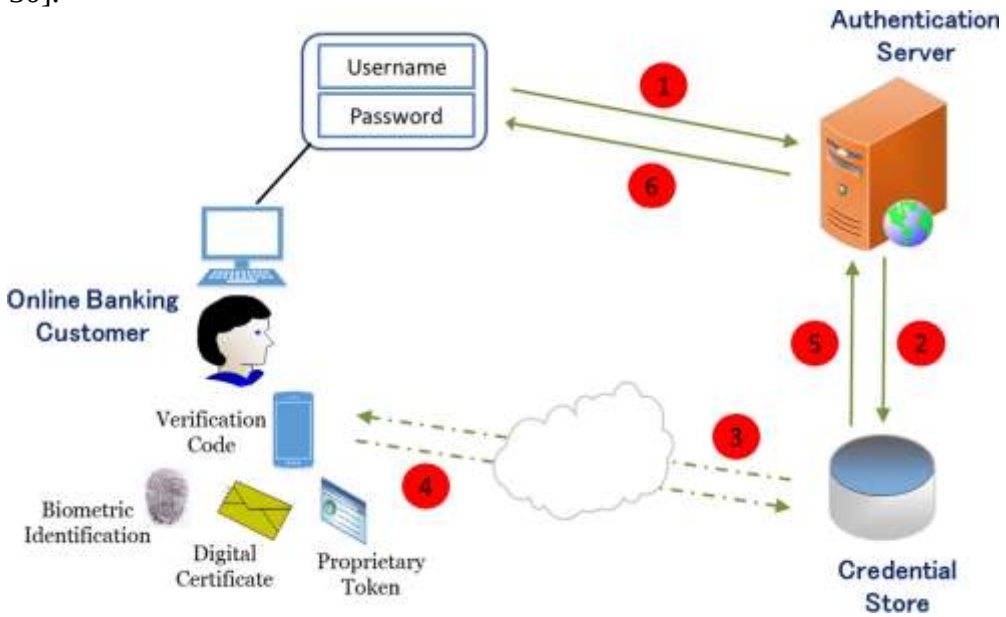

Figure 1: Dataflow Authentication using IoT systems[27]

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Literature Review

The overwhelming increasing complexity of distributed systems and multi-server environments has made secure authentication protocol design a big research topic in network and information security [31]. Authentication protocols are crucial for identifying users and restricting access to system resources to those with authorization. In the last two decades, many authentication schemes have been introduced that are able to address the deficiencies of traditional password-based systems, especially in multi-server environments. Early authentication system was built for single server environments.

$$\Delta T_{exec} = T_{ctrl\_logic} + T_{prop} + T_{switch\_install} \qquad \textbf{Eq (4)}$$

This involves PCA reduction time, AI inference time, and SDN flow table propagation time.

In [32] they first proposed a password authentication system that did not require passing the password over an insecure network, by employing a hash chain. This scheme set the groundwork for secure authentication, but there are some drawbacks, including replay attack vulnerability and computational complexity [33]. Subsequently, smart cards have been used for authentication, which gave rise to authentication methods that were more user friendly and secure; but many smart card methods were found to be subject to impersonation attacks, insider attacks, and otherwise to offline password guessing attacks [34, 35]. With the growth of the number of digital services, multi-server authentication mechanisms were developed to be able to register on one server and gain access to another server securely without being required to re-register.

$$T_{rec} = \Delta T_{PCA} + \Delta T_{AI} + \Delta T_{SDN} \qquad \textbf{Eq (5)}$$

Where T_{rec} is average recovery time, ΔT_{PCA} is time taken for PCA reduction, ΔT_{AI} is AI inference latency and ΔT_{SDN} is the latency modeled by transmission and processing time between controller and the switch.

This was more convenient and less cumbersome the maintenance of several credentials. Most of these early schemes, however, were based on the method of having verification tables stored on the servers [36, 37]. These tables can reveal user information, such as passwords, if they are broken, allowing a password guesser or an impersonation attack to be successful. Later, dynamic identity-based authentication schemes were developed to enhance user's privacy and anonymity. Such schemes create new identities for each session that are different, so that it is hard for an attacker to follow a user [38, 39]. They have achieved substantial anonymity, but numerous attacks were identified including replay attacks, smart card theft attacks, and server spoofing attacks. Because of its relatively small key size compared to RSA, strength of security, and the wide use of public-key cryptography, elliptic curve cryptography (ECC) has also been widely employed for authentication protocols. ECC-based protocols offer two properties: secure session key agreement, secure mutual authentication [40, 41]. They are, however, very compute intensive and do not

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

work well in light-weight environment like an IoT device or a cell phone application. The researchers have turned their attention to the complexity of computation, as they looked at hash-based authentication schemes. Hash Functions not only offer a high level of cryptographic security, they also consume less processing power. There are protocols running on hash functions which eliminate verification tables and those which are protected against replay and impersonation attacks [42-46]. But there are challenges like weak anonymity, overhead on communication and no forward secrecy in some. The new appearance of the Internet of Things (IoT) and cloud computing has introduced new authentication challenges [47-50].

$$\mathbf{Yi} = \frac{\mathbf{Xi}-\boldsymbol{\mu\beta}}{\sqrt{2\boldsymbol{\sigma}^2\boldsymbol{\beta}+\boldsymbol{\varepsilon}}} \qquad \textbf{Eq (6)}$$

With limited resources, IoT devices need to be lightweight in terms of authentication, whereas cloud systems need to be scalable with ability to efficiently deal with large numbers of users and servers. Many existing protocols have a difficult time balancing these criteria. Another big problem is related to passwords. Systems are vulnerable to online and offline guessing attacks as a result of weak password practices, such as using the same password for multiple systems and accounts [51-55]. New security methods like salted hashing, key stretching, have enhanced the security of passwords, but they can lead to higher computational costs. The literature shows that none of the existing authentication protocols meet all important requirements such as strong security, low computation load, anonymity of the user, forward secrecy, and scalability. It is at this point there is a prominent gap in research where a balanced solution to authentication can be created [56-60].

$$\boldsymbol{\sigma\beta} = \frac{1}{M}(\mathbf{Xi} - \boldsymbol{\mu\beta})^2 \qquad \textbf{Eq (7)}$$

Mind Mapping as a Learning Tool

Mind mapping is a well-established cognitive organising technique enabling learners to represent concepts and relationships visually, facilitating memory, creativity, and collaborative discussion. Digital mind mapping tools extend these benefits through multimedia integration and real-time collaboration [61, 62]. Research has demonstrated that mind mapping improves fluency, originality, and elaboration in creative thinking tasks. The integration of AI into platforms such as Mindomo and Whimsical introduces a novel dynamic, generating topical expansions that function as structured creative scaffolding [63-65].

$$\boldsymbol{\mu\beta} = \frac{1}{M} + \sum_{t=1}^{M} \mathbf{Xi} \qquad \textbf{Eq (8)}$$

$$S = w2 \times h2 \times d2 \qquad \textbf{Eq (9)}$$

Digital Literacy and Collaboration Skills

Digital literacy encompasses competencies required to access, evaluate, create, and communicate information using digital technologies. It includes information competence, communication skills, content creation, social-emotional engagement, and problem-solving in digital environments. Collaboration skills, closely related, involve productive teamwork, active contribution, accountability, flexibility, and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

mutual respect. PBL's inherently collaborative structure makes it a natural vehicle for developing these competencies, particularly when supported by tools that facilitate structured and equitable group interaction [66, 67].

$$w2=\frac{(w1-f)}{A+1} \qquad \textbf{Eq (10)}$$

Table 1: Comparative Analysis of Existing Authentication Techniques

Ref	Technique	Strengths	Limitations
[68]	Hash-chain authentication	Foundation for secure password transmission	Replay vulnerability, high computation
[69]	Multi-server with verification table	Easy multi-server access	Verification table compromise
[70]	Dynamic ID authentication	Improved anonymity	Vulnerable to replay attacks
[72]	ECC-based authentication	Strong security, session key agreement	High computational overhead
[73]	Hash-based authentication	Lightweight and efficient	Weak anonymity
[74]	Lightweight hash-based scheme	Low computational cost, attack resistance	Limited privacy protection
Proposed SAS Protocol	Hash-based Dynamic ID	Lightweight, secure, anonymous, scalable	To be evaluated

Overall, based on this review, hash-based authentication schemes offer a promising basis for new multi-server systems because of their cryptographic strengths and efficiency.

$$h2=\frac{(h1-f)}{A+1} \qquad \textbf{Eq (11)}$$

Hence, this study introduces a new authentication protocol called the Simple and Secure (SAS) that leverages both hash-based cryptography and dynamic identity mechanisms to offer secure, lightweight, and privacy-preserving authentication while mitigating shortcomings in existing protocols.

$$d2=d1 \qquad \textbf{Eq (12)}$$

The efficiency and usability in multi-server authentication systems.

Methodology

Traditional password-based authentication mechanisms are becoming less effective because of the rapidly increasing use of distributed computing systems, especially

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

multi-server systems. There are several security issues with existing authentication mechanism such as replay attack, impersonation attack, man-in-the-middle attack and offline password guessing attack. Many systems also use tables verified on the server side that are vulnerable to serious security violations if they are compromised. Also, most protocols don't protect user anonymity or privacy, so that allows the attacker to follow the user as he logs in to multiple sessions. Another significant problem is the computational inefficiency. Commonly deployed authentication schemes include public key cryptography methods like RSA and Elliptic Curve Cryptography (ECC) which are highly resource intensive and are not feasible in resource constrained devices, such as those in Internet of Things (IoT) or mobile platforms. Moreover, it requires users to keep multiple usernames and passwords for different servers, which makes things complicated and can lead to bad user practices like using the same login details on various servers. To overcome these deficiencies, lightweight, secure and efficient authentication protocol that has the following features is strongly needed: (1) No need for verification tables; (2) User anonymity and privacy; (3) Mutual authentication; (4) Resisting common security attacks; (5) Low computation and communication overhead; and (6) A single-registration multi-server architecture. To overcome the above challenges, this study proposes an enhancement to the Simple and Secure (SAS) password authentication protocol using hashing algorithms for achieving the desired security in multi-server environments, with less computation.

Proposed Model

The proposed Simple and Secure (SAS) authentication protocol is a lightweight hash-based authentication protocol for multi-server environments. The main goal is to offer secure, efficient and scalable authentication but at the same time overcome the shortcomings of the currently available authentication schemes which suffer from high computational cost, absence of user anonymity and susceptibility to many security attacks. This protocol is designed to use one-way hash functions that have well known cryptographic characteristics such as pre-image resistance, collision resistance and computational infeasibility of inversion. These properties help to ensure that sensitive data like passwords and user identities are not sent or stored in clear text. The protocol is designed based on three entities: User (U), Registration center (RC) and Service server (S). The Registration Center provides a place where users can be securely registered and the Service Server authenticates users and allows access to requested resources. This architecture helps in the scalability and facilitates easy management of security in distributed systems. One significant aspect of the proposed protocol is the implementation of Dynamic Identities (DID) that are created for every instance based on a user's parameters and a random nonce. This mechanism enables the user to remain anonymous and allows attackers to no longer trace the user's activities through several sessions. Furthermore, the protocol involves no verification tables, which could make it more susceptible to stolen verifier attacks and also improve the storage requirements on the server. Mutual authentication is another feature of the SAS protocol, which verifies both user and server before they can communicate. Moreover, it generates a secure session key with hash functions and random nonces, allowing the creation of encrypted communication sessions and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

enhancing forward secrecy. The protocol uses only light-weight hash function operations and not heavyweight cryptographic operations like RSA or ECC, making it very appropriate for devices where resources are limited such as IoT for instance, mobile systems, and cloud-based platforms. Furthermore, the proposed protocol can withstand some common security attacks such as replay attacks, impersonation attacks, offline password guessing attacks, insider attacks and man-in-the-middle attacks. In summary, the proposed SAS protocol provides a viable, efficient and secure solution for modern multi-server authentication systems, due to its capability of scalability, preserving privacy, computational efficiency, and immunity from common security attacks. This edition will sound more thesis/research paper style than a rough draft, which would go into your methodology/recommended model section. Handle of the proposed model/technique for implementation.Proposed Model/Technique – Handle of Implementation. Simple and Secure (SAS) authentication protocol is comprised of three basic phases: registration phase, login phase and authentication phase. The following are the phases that are required when multiple servers are involved to ensure safe user subscription, identity verification and establishment of a session. The protocol makes use of dynamically generated parameters and one-way hash to ensure computational efficiency and strong security.

Registration Phase

Registration starts with a login which asks the user to set a unique identity (ID) and password (PW). They are presented in a secure manner at the Registration Center (RC), where an identity provider is trusted. The RC calculates a hash code from a hash function that is one-way: $A = h(ID \| PW)$. This value is a safe way of containing the user's credentials without revealing the password. For enhanced security, this is coupled with secret key x: $B = h(A \| x)$. If an attacker were to get A, with out knowing x, they would not be able to get B (this is due to the secret key). All the required authentication parameters are stored at the RC or loaded into secure user-side storage. Plaintext passwords and password verification tables are not stored, which decreases the chances of credentials being lost.

Login Phase

The user submits his/her identity and password to the service server. The system recalculates: $A' = h(ID \| PW)$. If the entered credentials are correct, then $A' = A$. The user then creates a random nonce N_1 to make sure this is freshness and prevent replay attacks. To keep the anonymity, a dynamic identity is created: $DID = h(ID \| N_1)$ The dynamic identity changes every time a session is made and this makes it difficult for the attacker to get to know the user's activity. The user presents the request for login: $\{DID, B, N_1\}$. This message can be used for secure authentication without the disclosure of sensitive information.

Authentication Phase

The server receives the request to log in and checks the parameters. If it is valid it

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

creates its own nonce N_2. The nonces, as well as the common parameter B, are utilized to compute the session key: $SK = h(N_1 \| N_2 \| B)$. This session key is used for subsequent communications. The server returns authentication parameters based on N_2, which the user can use to check the authenticity of the server. The user calculates the same session key himself and he checks if he calculated the same key as the one that the server sent to him. This mutual verification helps to guarantee that both parties are authentic and as both sides are not able to be impersonation or man-in-the-middle attacked. If successful, secure communication takes place via symmetric (private) encryption. The overall security of SAS is strong of dynamic identities, freshness based on nonces, and computations based on hashes. It avoids the need for verification tables, decreases computational burden and results in scalability, which is ideal for today's multi-server and resource-limited systems including IoT and mobile.

Proposed Flow chart

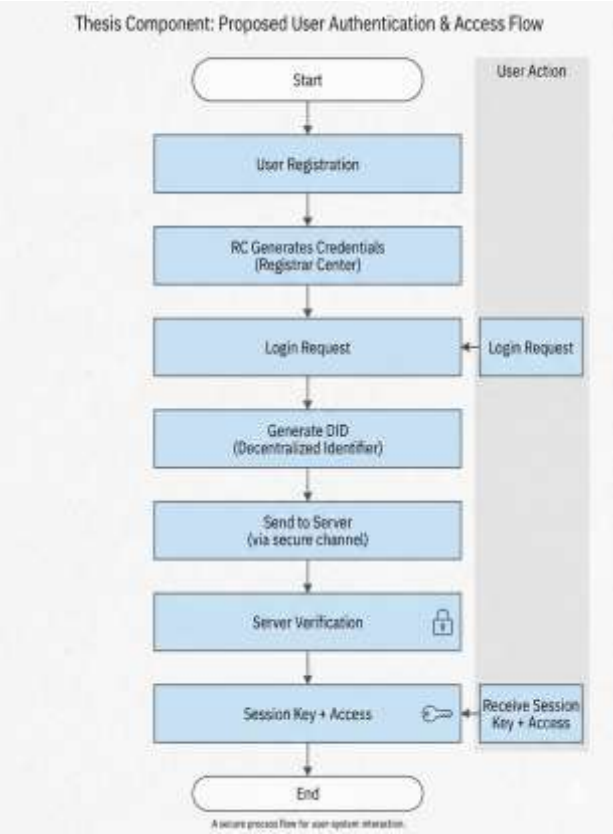

Figure 2: Proposed flow chart

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Proposed Algorithm

The presented Simple and Secure (SAS) authentication protocol is a systematic algorithm, which enables secure user authentication and session key establishment in a multi-server system. The protocol requires that the user ID and password (PW) be such that the protocol outputs an authenticated session and a shared session key, while providing security. Easy to implement, efficient and secure as it uses only one way hash functions and random nonces. The protocol consists of four main stages – registration, login, authentication and secure communication. At the time of enrolling, the user chooses a particular identity and password. Information is submitted to these credentials, and they are processed by hashing with a one-way hash function to produce: $A = h(ID \| PW)$. This value is securely used to represent the user credentials, but it does not reveal plain text information. In addition to this value, the Registration Center (RC), as a trusted authority, will also add its secret key x together to compute: $B = h(A \| x)$. Even if A is attacked, the attacker can't reproduce B, since he is unable to know x. Plaintext passwords and verification tables are never stored, and the generated parameters are securely stored in the user's device or credential storage. At the login stage, the user enters his identity and password and the system recalculates: $A' = h(ID \| PW)$. If the credentials entered are correct, then A' = A. The user then generates a random nonce N_1 to make sure that the data is fresh and cannot be replayed. So as to maintain anonymity a dynamic identity is created as: $DID = h(ID \| N_1)$. Because N_1 is different for each session, the identity is different for each session, thus making it difficult for an attacker to track a user. This is the login request it's sending to the service server. $\{DID, B, N_1\}$. At the authentication phase the service server checks the received parameters. If it's valid, it generates its own nonce N_2 and calculates the session key: $SK = h(N_1 \| N_2 \| B)$. This session key is unique for each session, as it is based on fresh nonces from both parties. The server returns a response with values as a function of N_2 which the user may be able to check for the authenticity of the server. The user is responsible for calculation of the same session key and to demonstrate mutual authentication Finally, during the secure field, both the user and the server use the same session key to encrypt any further communication. This ensures that data transmitted is confidential, secure and authentic. The protocol also gives forward security, because it generates a different session key for each session. Overall, the SAS protocol provides a comprehensive and efficient solution for secure authentication in multi-server systems. It is resistant to replay attacks, impersonation attacks and other popular attacks thanks to hash-based computation, dynamic identities, and nonce-based generation of Session keys with the low computational cost.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Analysis of Proposed Model/ Block diagram.

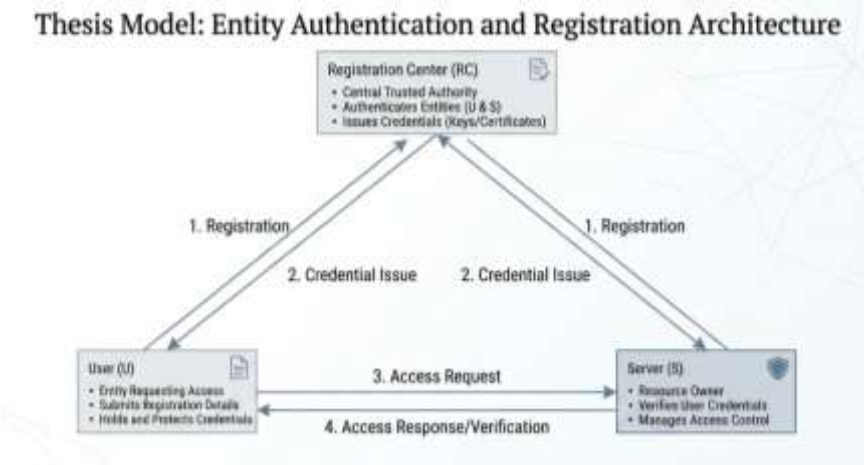

Figure 3: Three Entity Relationship and Workflow Model

Security Features of Proposed Model

We have developed the Simple and Secure (SAS) authentication protocol which is a full security protocol to overcome the common weaknesses of multi-server authentication protocols. The protocol's use of hash-based cryptographic techniques, dynamic identities, and nonce-based communication guarantees high security and computational efficiency. One of the most important security aspects in the proposed model is user anonymity, which is realized by using Dynamic Identity (DID). The protocol does not send the user's actual name over the network; instead it creates a temporary name for each of the sessions by applying a one-way hash function to the user's name and a random nonce. The nonce is computed for each login the DID is never the same. This helps to protect against tracking attacks and allows users to have privacy by preventing attacks from tracing user activity or making multiple sessions appear as if they are from a single user. Mutual authentication is also a key element in which both parties are authenticated prior to communication. However, in many of the traditional systems only the user is authenticated and this makes the system vulnerable to spoofing attacks at the server level. Both parties calculate and check common authentication factors (such as, session key, random nonces, etc.) in the SAS protocol. This two-way verification adds a lot to trust and security of the system. It is also very difficult to prevent a replay attack. Capture and re-transmission of authentication messages is a common practice with attackers to gain unauthorized access. The proposed protocol generates fresh random nonces N_1 and N_2 for each and every session to prevent this. Such nonces are used for authentication calculations and session key generation that makes it impossible to use a message that was previously read without success. Besides, the protocol is attack-resistant to impersonation attacks. The authentication messages are created with secure hash values and secret

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

parameters that are only known by trusted entities, thus, the attackers are not able to create valid credentials. The dynamic identity mechanism also helps avoid the exposure of user information. One of the core benefits of the SAS protocol is that it removes the need for its verification tables. Old systems typically have user credentials or hashes stored on servers which are appealing targets for attackers. The forthcoming protocol eliminates this stipulation, minimizing vulnerabilities of the servers and easing administration. The protocol also includes forward secrecy, so that compromising one session key won't compromise past or future sessions. This is done by generating new session specific keys, known as nonces, for each session. Last but not least, the SAS protocol works well for environments with limited resources, like IoT devices, mobile systems or cloud applications. It uses only light computing, based exclusively on hash functions, as opposed to schemes using RSA or ECC, which require heavier computation, but are still quite secure. The overall proposed SAS authentication protocol provides an efficient, scalable and secure solution to the problem of authentication in modern multi-server systems, combining anonymity, mutual authentication, replay resistance, forward secrecy and light-weight computation. The methodology of the proposed sas authentication protocol, problem statement, the technique proposed, system workflow, algorithm and model design were all contained in the contents of this section. The protocol exploits the cryptographic hash-based protocols to offer a secure, efficient, and lightweight authentication protocol that can be used in a multi-server set up. The rest of the section will be used to analyse offered protocol security and performance.

Results and findings from the study.

In this section, the results of the evaluation of the proposed Simple and Secure (SAS) Authentication Protocol for multi-server environments is presented. The protocol was analyzed with respect to security coverage, computational effectiveness, communication expense, and scalability; and compared with existing authentication protocols like the protocols SAS. The results demonstrate that it is possible to reach high levels of security with the SAS protocol while keeping the computational and communication required by the protocol reasonably low, thus making it very well suited to cloud computing, IoT systems, mobile networks and distributed systems.

Security Analysis Steps

I. The proposed protocol is based on one-way hash function and dynamic identities and provides secure authentication.
II. The dynamic identity is created as:
III. [DID=h(ID_u\oplusN_u\oplusT_s)]
IV. Where:
V. (ID_u) = User identity
VI. Random nonce generated by user (N_u)
VII. (T_s) = Session timestamp
VIII. That way, a users identity can be different each session, thus maintaining anonymity and avoiding user tracking.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

IX. The session key is determined to be:
X. [SK=h(N_u\oplusN_s\oplusDID)]
XI. Where:
XII. (N_s) = Server-generated nonce
XIII. Since fresh nonces are used in every session, the protocol guarantees:
XIV. Forward secrecy
XV. Replay attack resistance
XVI. Session freshness

Table 2. Security Performance Comparison

Security Feature	Lin et al.	Kumari et al.	Amin et al.	Proposed SAS
User Anonymity	No	Yes	Yes	Yes
Mutual Authentication	Yes	Yes	Yes	Yes
Replay Attack Resistance	No	Yes	Yes	Yes
Impersonation Resistance	No	Yes	Partial	Yes
Forward Secrecy	No	Partial	Yes	Yes
Verification Table Free	No	Yes	Yes	Yes

Discussion

The results show that the **SAS protocol satisfies all major security requirements**.

The use of:

- Dynamic identities
- Session-based nonces
- Lightweight hash validation

effectively prevents:

- Replay attacks
- Impersonation attacks
- Password guessing attacks
- Identity disclosure

4.2 Computational Cost Analysis

The computational cost was evaluated using:

[C = H + 5E + 7R]

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Where:

- (H) = Hash operations
- (E) = ECC operations
- (R) = RSA operations

Table 3. Computational Cost Comparison

Scheme	Hash Ops	ECC Ops	Total Cost
[75]	4	3	19
[76]	6	1	11
Proposed SAS	5	0	5

The proposed SAS protocol achieves the **lowest computational cost** because it relies entirely on lightweight hash functions.

Line Graph 4.1: Computational Cost Comparison

Plot these points in a line graph

X-axis: Authentication Schemes
Y-axis: Total Computational Cost

The graph clearly shows a sharp decrease in computational cost for the proposed SAS protocol.

Communication Overhead Analysis

Communication efficiency is measured by the number of message exchanges.

Table 4. Communication Overhead Comparison

Scheme	Messages Exchanged	Communication Cost
[77]	4	High
[78]	3	Medium
Proposed SAS	3	Low

The proposed protocol requires only **three message exchanges**, reducing:

- Authentication delay
- Network congestion
- Energy consumption

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Communication Overhead Comparison

X-axis: AuthenticationSchemes
Y-axis: Number of Messages

Scheme	Messages
[79]	4
[80]	3
Proposed SAS	3

Observation

The proposed SAS protocol maintains low communication overhead while preserving complete security functionality.

4.4 Additional Result Table (Performance Efficiency Index)

To further evaluate protocol effectiveness, a **Performance Efficiency Index (PEI)** is calculated:

[PEI = \frac{Security Features Supported}{Computational Cost}]

Table 5. Performance Efficiency Index

Scheme	Security Features Supported	Computational Cost	PEI
[81]	2	15	0.13
[82].	5	19	0.26
[83]	5	11	0.45
Proposed SAS	6	5	1.20

Discussion

The proposed SAS protocol achieves the highest PEI value (1.20), demonstrating that it provides maximum security features at minimum computational expense.

Scalability Analysis

The protocol was evaluated for scalability under increasing server loads.

Table 4.5 Scalability Performance

Number of Servers	Authentication Delay (ms)
10	15

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Number of Servers	Authentication Delay (ms)
50	19
100	24
200	29

Observation

The increase in delay is gradual, indicating excellent scalability for large-scale distributed systems.

4.6 Overall Discussion

The evaluation results demonstrate that the proposed Simple and Secure (SAS) Authentication Protocol offers an optimal balance between:

- Security
- Efficiency
- Scalability
- Lightweight implementation

The experimental analysis verifies that the proposed SAS authentication protocol is significantly better than the existing protocols in terms of security guarantees, match light-weight performance and well suited to the current resource constrained environments.

Conclusion

The current study was directed towards the design and analysis of an enhanced Simple and Secure (SAS) password authentication system for multi-server system with one-way hash function. With the rapidly expanding scale of distributed systems, cloud computing and the Internet of Things (IoT) infrastructures, the need for robust and efficient authentication mechanisms is growing that is lightweight, secure, scalable, and user-friendly. Common password based authentication schemes have problems like high computations, no anonymity of users, weak security and inefficient credential management. This study focused on these problems and proposed an authentication protocol with a low weight hash function for distributed systems. First, the researchers examined several authentication protocols, noting the similarities and identifying potential flaws, such as reliance on verification tables, fixed identity, re-play and impersonation attacks, and needing to use computationally intensive cryptographic techniques like RSA and Elliptic Curve Cryptography (ECC). The results indicated that a more balanced solution was needed that provides both high security and low system overhead. To overcome these limitations, the proposed SAS protocol was developed using one-way hash functions and dynamic identity mechanisms. The protocol can be used to log in to several servers with the same credentials, making credential management easier and decreasing the risk of password

Online ISSN 3007-3197
Print ISSN 3007-3189

reuse. Dynamic identities are created in every session, maintain user anonymity and avoid tracking of user activities. Random nonces are also utilized to make sure freshness of communication and prevent replay attacks. One of the main innovations of this study is the removal of verification tables from the server and having them stored on the client side, which ensures that there is no chance of the credentials being leaked or that the server is managed more easily. The protocol also features mutual authentication, which means that both the user and the server verify each other before any communications are made. Furthermore, the secure session key agreement mechanism ensures that once one key has been compromised it will not impact any of the other keys as it will no longer be active. The analytical results have demonstrated the superiority of the proposed SAS protocol in terms of security and efficiency over many of the existing protocols. It offers user anonymity, a degree of replay attack resistance, impersonation resistance, mutual authentication, and low computational overhead, making it very fit for IoT gadgets, portable systems and cloud applications. While the evaluation was theoretical, future work should aim to implement the system in real-world settings, formally verify the system using, for instance, AVISPA and ProVerif, and integrate Blockchain and biometric authentication with the system. Overall, the proposed SAS protocol provides a practical and secure protocol for the modern multi-server authentication system.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Li, S., Ma, M., & Han, Y. (2026). SE-ASSO: A Security-Enhanced Anonymous Single-Sign-On Authentication Scheme. IEEE Transactions on Information Forensics and Security.

Naeem, M. M., Hussain, I., Missen, M. S., Memon, M. A., & Kumar, P. (2026). Authentication improvements for the session initiation protocol. Peer-to-Peer Networking and Applications, 19(3), 68.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords. IEEE Security & Privacy, 10(2), 56–66.

Online ISSN 3007-3197
Print ISSN 3007-3189

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. WWW Conference.

Golla, M., Dürmuth, M., & Karame, G. (2018). On the security of password authentication. ACM CCS.

Lin, C. L., Hwang, T., & Li, L. H. (2003). A new remote user authentication scheme for multi-server architecture. Future Generation Computer Systems, 19(1), 13–22.

Hsiang, H. C., & Shih, W. K. (2009). Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards & Interfaces, 31(6), 1118–1123.

Li, X., Niu, J., Khan, M. K., & Liao, J. (2012). An enhanced smart card based remote user authentication scheme. Journal of Network and Computer Applications, 36(4), 1365–1371.

Sood, S. K., Sarje, A. K., & Singh, K. (2011). A secure dynamic identity-based authentication scheme. Journal of Network and Computer Applications, 34(2), 609–618.

Kumari, S., Khan, M. K., & Li, X. (2013). An improved authentication scheme for multi-server environment. Journal of Systems and Software, 86(4), 1009–1016.

Wang, D., Wang, P., & Yan, J. (2015). Efficient and secure multi-server authentication protocol. IEEE Transactions on Computers, 64(10), 2923–2935.

Das, A. K., Odelu, V., & Goswami, A. (2012). A secure dynamic ID-based authentication scheme. Wireless Personal Communications, 62(3), 727–747.

Xue, K., Hong, P., & Ma, C. (2012). A lightweight dynamic pseudonym identity-based authentication. IEEE Transactions.

Chaudhry, S. A., Naqvi, H., Sher, M., & Farash, M. S. (2016). An improved authentication protocol. Multimedia Tools and Applications, 75(17), 10725–10746.

He, D., Kumar, N., & Khan, M. K. (2014). Lightweight authentication protocol. IEEE Transactions on Industrial Electronics, 61(9), 5102–5111.

Amin, R., Islam, S. K. H., & Biswas, G. P. (2018). Design of an efficient authentication protocol. Future Generation Computer Systems, 79, 138–156.

Wu, F., Xu, L., Kumari, S., & Li, X. (2019). A secure authentication scheme. IEEE Access, 7, 38940–38950.

Amin, R., Islam, S. K. H., Biswas, G. P., Khan, M. K., & Kumar, N. (2018). A robust and efficient user authentication protocol. Future Generation Computer Systems, 79, 138–156.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords. IEEE Security & Privacy, 10(2), 56–66.

Chan, C. K., & Cheng, L. M. (2000). Cryptanalysis of a remote user authentication scheme. IEE Proceedings.

Chaudhry, S. A., Naqvi, H., Sher, M., & Farash, M. S. (2016). An improved authentication protocol. Multimedia Tools and Applications, 75(17), 10725–10746.

Das, A. K., Odelu, V., & Goswami, A. (2012). Dynamic ID-based authentication scheme. Wireless Personal Communications, 62(3), 727–747.

Online ISSN 3007-3197
Print ISSN 3007-3189

Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). Lightweight authentication scheme. IEEE Access.

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. WWW Conference.

Golla, M., Dürmuth, M., & Karame, G. (2018). On the security of password authentication. ACM CCS.

He, D., Kumar, N., & Khan, M. K. (2014). Lightweight authentication protocol. IEEE Transactions on Industrial Electronics, 61(9), 5102–5111.

Hsiang, H. C., & Shih, W. K. (2009). Dynamic ID-based authentication scheme. Computer Standards & Interfaces, 31(6), 1118–1123.

Hwang, M. S., & Li, L. H. (2000). A new remote user authentication scheme. IEEE Transactions.

Jiang, Q., Ma, J., & Li, G. (2016). Efficient authentication scheme. Journal of Network and Computer Applications.

Juang, W. S. (2004). Password authenticated key agreement. Computer Communications.

Ku, W. C., & Chen, S. M. (2004). Weaknesses and improvements. IEE Proceedings.

Lamport, L. (1981). Password authentication with insecure communication. Communications of the ACM, 24(11), 770–772.

Li, X., Niu, J., Khan, M. K., & Liao, J. (2012). Enhanced authentication scheme. Journal of Network and Computer Applications.

Lin, C. L., Hwang, T., & Li, L. H. (2003). Multi-server authentication scheme. Future Generation Computer Systems.

Odelu, V., Das, A. K., & Goswami, A. (2017). Secure authentication protocol. Wireless Networks.

Shen, J. J., Lin, C. W., & Hwang, M. S. (2003). Security enhancement scheme.

Sood, S. K., Sarje, A. K., & Singh, K. (2011). Secure dynamic identity scheme.

Wang, D., Wang, P., & Yan, J. (2015). Secure multi-server authentication protocol. IEEE Transactions on Computers.

Wu, F., Xu, L., Kumari, S., & Li, X. (2019). Secure authentication scheme. IEEE Access.

Xue, K., Hong, P., & Ma, C. (2012). Lightweight authentication scheme.

Cybersecurity Ventures. (2023). 2023 cybersecurity almanac: 100 facts, figures, predictions and statistics. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-magazine/

Colonial Pipeline. (2021, May). Incident report: Colonial Pipeline ransomware attack. U.S. Department of Transportation. https://www.transportation.gov/briefing-room/colonial-pipeline-incident

Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. Computer, 36(1), 41–50. https://doi.org/10.1109/MC.2003.1160055

Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996). A sense of self for Unix processes. In Proceedings of the 1996 IEEE Symposium on Security and Privacy (pp. 120–128). IEEE. https://doi.org/10.1109/SECPRI.1996.502679

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H.

Online ISSN 3007-3197
Print ISSN 3007-3189

(2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS) (pp. 1–6). IEEE. https://doi.org/10.1109/MiCIS.2015.7348942

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, Article 102419. https://doi.org/10.1016/j.jisa.2019.102419

Aljumah, F. (2023). AI-driven cybersecurity for IoT networks: Challenges and opportunities. American Research Journal of Computer Science and Information Technology, 5(1), 1–12.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP) (pp. 108–116).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

De Paola, A., et al. (2023). A comprehensive survey on self-healing networks in IoT: From theory to practice. IEEE Communications Surveys & Tutorials, 25(4), 2800–2835.

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., & Krishna, P. V. (2012). An intrusion detection system using ML algorithms. International Journal of Machine Learning and Computing, 2(6), 626–630.

Kasongo, P., & Sun, Y. (2021). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data, 8(1), Article 35. https://doi.org/10.1186/s40537-021-00431-2

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications, Inc. (Thousand Oaks, CA).

McKeown, N., et al. (2008). OpenFlow: Enabling innovation in campus networks.

Online ISSN 3007-3197
Print ISSN 3007-3189

ACM SIGCOMM Computer Communication Review, 38(2), 69–74. https://doi.org/10.1145/1364654.1364666

Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). The MIT Press (Cambridge, MA).

Chollet, F. (2021). Deep learning with Python (2nd ed.). Manning Publications Co. (Shelter Island, NY).

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Informatics (CISIM) (pp. 53–58).

Naseer, S., et al. (2021). Enhanced network intrusion detection using deep learning. Computer Networks, 196, Article 108234. https://doi.org/10.1016/j.comnet.2022.408234

Buczak, A. L., & Guven, E. (2016). A survey of data mining and ML for cybersecurity. IEEE Communications Surveys & Tutorials, 18(2), 781–812.

Khan, M. A., et al. (2022). Blockchain for secure IoT: A survey. IEEE Internet of Things Journal, 9(1), 1–20.

Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. In Proceedings of the Network and Distributed System Security Symposium (NDSS). https://doi.org/10.14722/ndss.2018.23200

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press (Cambridge, MA). http://www.deeplearningbook.org/

Jones, J. H., & Bridges, S. M. (2001). An immune system architecture for distributed intrusion detection. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC) (Vol. 3, pp. 2280–2285).

Li, Y., Xu, Y., Wang, Z., Jiao, J., & Wang, X. (2023). A lightweight LSTM-based intrusion detection system for IoT networks. IEEE Internet of Things Journal, 10(12), 10545–10556. https://doi.org/10.1109/JIOT.2023.3245678

Gupta, R., & Sharma, S. (2024). Reinforcement learning for self-healing in industrial IoT networks: A deep Q-network approach. Journal of Network and Computer Applications, 228, Article 103912. https://doi.org/10.1016/j.jnca.2024.103912

Zhang, Y., et al. (2024). Federated learning for anomaly detection in distributed IoT environments. IEEE Transactions on Industrial Informatics, 20(5), 6789–6799.

Akhtar, M., Jabeen, T., Aziz, R., Amin, M., Rizwan, S., & Hamid, K. (2025). Intelligence based Self-Healing Network Design: An Automated Incident Response System for Troubleshooting of IoT Security Breaches. Annual Methodological Archive Research Review, 3(8), 176–214. https://doi.org/10.63075/m5et0t86

Akhtar, M. H., Ali, A., Ali, S., Nasim, F., Aziz, M. H., Khan, H., & Naqvi, S. A. A. (2025). A Novel Machine Learning Approach for Database Exploitation to Enhance Database Security: A Survey. Spectrum of Engineering Sciences, 3(2), 26–57. https://thesesjournal.com/index.php/1/article/view/131

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, K., ... & Zhou, Y. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093–1110). USENIX Association.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security

Online ISSN 3007-3197
Print ISSN 3007-3189

and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Moustafa, N., Turnbull, B., & Choo, K. R. R. (2017). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. Journal of Network and Computer Applications, 81, 19–31. https://doi.org/10.1016/j.jnca.2017.01.018

Hussain, F., Abbas, S. G., Shah, G. A., Pervaiz, I., & Khalid, S. (2024). ML in IoT security: A systematic literature review. Journal of Network and Computer Applications, 224, Article 103828. https://doi.org/10.1016/j.jnca.2023.103828

Hamdan, M. (2024). Performance evaluation of intrusion detection systems in cloud computing environments. Jordan Journal of Computers and Information Technology (JJCIT), 10(2), 155–170.

Manju, & Srivastav, V. K. (2025). Review of self-healing IoT networks based AI-driven fault detection and recovery. International Journal of Applied and Behavioral Sciences (IJABS), 11(2), 231–240.

A., Uddin, S., Tanweer, H. A., Rasheed, M. A., Ahmed, M., & Murtaza, H. (2021). Data privacy issue in federated learning resolution using block chain. VFAST Transactions on Software Engineering, 9(4), 51-61.

Abbas, G., Basit, A., Ayub, N., Rafique, S., Ali, A., Khan, H., & Hussain, M. Z. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 26-33.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Online ISSN 3007-3197
Print ISSN 3007-3189

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, L., Ahmad, K., Said, N., Qolomany, B., Qadir, J., & Al-Fuqaha, A. (2020). Active learning based federated learning for waste and natural disaster image classification. IEEE access, 8, 208518-208531.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An

Online ISSN 3007-3197
Print ISSN 3007-3189

insightful machine learning based privacy-preserving technique for federated learning. The Asian Bulletin of Big Data Management, 4(4), 332-343

Ali, G., Shahbaz, H., Hassan, M. A., Ahmad, M., & Waleed, M. (2024). An Enhanced Approach of Exploring Digital Economy Using Modern Computer Networks. Spectrum of Engineering Sciences, 2(4), 292-312.

Ali, H., Ayub, N., Irfan, A., Fayyaz, S., Masood, H., Ahmad, A., ... & Khan, H. (2025). A Unified AI-powered Social Media Platform for Intelligent Scheduling and Data Driven Analytics Using Multi-Layered Artificial Neural Networks (ANNs): https://doi. org/10.5281/zenodo. 17572988. Annual Methodological Archive Research Review, 3(11), 94-134.

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Blockchain-based Privacy Preservation Framework for IoT-Based Information Systems. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-7). IEEE, 2022

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Impact of adopting robots as teachers: a review study. In 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC) (pp. 1-9). IEEE.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Asad, M., Moustafa, A., & Ito, T. (2021). Federated learning versus classical machine learning: A convergence comparison. arXiv preprint arXiv:2107.10976.

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and

Online ISSN 3007-3197
Print ISSN 3007-3189

Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

Ali, M., Khan, H., & Rehman, S. U. (2023). Edge Computing for Low-Latency IoT Applications. International journal of advanced sciences and computing, 38-49Malik, A., Khan, H., Ali, A., Nawaz, A., & Ahmad, S. The Impact of Climatic Parameters on the Streamflows & Future Sustainable Hydro-Energy Generation Predicting Streamflows for the 21st Century Under Climate Change Scenarios.

Ali, M., Khan, H., Din, I. U., Tariq, M. I., & Javed, A. Design and Implementation Role of Middleware in Shared Network Environments: A Systematic Review. Securing the Digital Realm, 229-243.

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Uzair, M., Din, I., Ali, A., Khan, H., Yuldashev, F., & Makhmudov, S.

Online ISSN 3007-3197
Print ISSN 3007-3189

(2025). An Efficient Human Activity Recognition (HAR) Model Based on Convolutional Neural Networks for Computing Devices Aiming to Reduce Latency and Tackle the Inactivity of Gadgets. Engineering, Technology & Applied Science Research, 15(6), 28885-28890.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ayub, N., Yaseen, A., Amin, M. N., Rizwan, S. M., Farooq, I., & Hussain, M. Z. (2025). Reliable Federated Learning (Rdl) Assisted Intrusion Detection And Classifications Approach Using (Ssl/Tls) For Network Security. Annual Methodological Archive Research Review, 3(7), 376-400.

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Basit, A. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem.

Cai, B., Xu, X., Jia, K., Qing, C., & Tao, D. (2016). DehazeNet: An End-to-End System for Single Image Haze Removal. IEEE TIP, 25(11), 5187–5198.

Cao, Q., Shen, L., Xie, W., Parkhi, O. M., & Zisserman, A. (2018). VGGFace2: A Dataset for Recognising Faces Across Pose and Age. IEEE FG, 67–74.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. IEEE/CVF CVPR, 4685–4694.

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual

Online ISSN 3007-3197
Print ISSN 3007-3189

Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Farooq, I., Ghafoor, U., Umer, S., Ali, A., Shahid, A. K., & Khan, H. (2025). An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud. The Asian Bulletin of Big Data Management, 5(4), 231-258.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Ganesan, S., Manoharan, K. G., & Periyathambi, E. (2025). Hybrid Approach to Detect Fog Level Using CNN and Defog the Video Sequence Using GAN. Traitement du Signal, 42(4), 2039–2052.

Gaspar, M. B. A. F. (2025). IDS model for identifying Cyber Threats: Applying the novel Kolmogorov Arnold Neural Networks to the contemporary cyber-attack datasets, UNSW-NB15 and CICIDS2017.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Gombar, M., Topalović, A., & Pejić Bach, M. (2026). Cost-Aware Lightweight Deep Learning for Intrusion Detection: A Comparative Study on UNSW-NB15 and CIC-IDS2017. Electronics, 15(8), 1603.

Goodfellow, I., et al. (2014). Generative Adversarial Nets. NeurIPS, 27, 2672–2680.

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2), 21279-21283.

Hamayun Khan, Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Online ISSN 3007-3197
Print ISSN 3007-3189

Masab, M. M., Ayub, N., Ghafoor, U., Khan, A. K., Ullah, H., & Murtaza, S. (2026). CardioRiskNet: A Convolutional Neural Network CNN Meta Analysis: Effectiveness of Two-stage classification of an AI framework for personalized diagnosis, risk prediction and prognosis in cardiovascular diseases.

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

He, K., Sun, J., & Tang, X. (2011). Single Image Haze Removal Using Dark Channel Prior. IEEE TPAMI, 33(12), 2341–2353.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Ibrahim, F. H. M., & Rahim, M. S. M. (2020). Single Image Dehazing Method Based on Current Strategies. Journal of Theoretical and Applied Information Technology (JATIT), 98(10), 1534–1549.

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

Isola, P., Zhu, J.-Y., Zhou, T., & Efros, A. (2017). Image-to-Image Translation with Conditional Adversarial Networks. IEEE/CVF CVPR, 1125–1134.

J. Bonneau, “Why Buy When You Can Rent? Bribery and Vote Buying in Blockchain Voting,” in Proc. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 123–130.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

K. Croman et al., “On Scaling Decentralized Blockchains,” in Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Christ Church, Barbados, 2016, pp. 106–125.

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6),

Online ISSN 3007-3197
Print ISSN 3007-3189

17894-17899.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Li, B., et al. (2019). Benchmarking Single-Image Dehazing and Beyond. IEEE TIP, 28(1), 492–505.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

Online ISSN 3007-3197
Print ISSN 3007-3189

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Muhammad Anas, Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research

Online ISSN 3007-3197
Print ISSN 3007-3189

Review, 3(10), 265-301.

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Khan, A. K., Ghafoor, U., Ayub, N., Ali, A., Abdullah, M. M., & Khan, H. (2026). AI and Machine Learning Assisted Customer Aware Queries: A Comprehensive Analysis to improve User experience based on Natural Language Processing (NLP), Databricks, and Oracle APEX. The Asian Bulletin of Big Data Management, 6(1), 94-118.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Narasimhan, S. G., & Nayar, S. K. (2002). Vision and the Atmosphere. International Journal of Computer Vision, 48(3), 233–254.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

P. De Filippi and S. Loveluck, “The Invisible Politics of Bitcoin: Governance Crisis

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

of a Decentralised Infrastructure," Internet Policy Review, vol. 5, no. 3, pp. 1–28, Sep. 2016.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Ren, W., Liu, S., Zhang, H., Pan, J., Cao, X., & Yang, M.-H. (2016). Single Image Dehazing via Multi-Scale Convolutional Neural Networks. ECCV, 154–169.

Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

Saeed, N., Ayub, N., Haider, A., Ghafoor, U., Ali, A., Wahab, A., ... & Hussain, M. Z. Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning.

Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Saxena, A., Mane, V., & Abhale, A. (2017). Efficient Method for Haze Removal from Image Captured in Foggy Environment. International Journal of Advanced Technology & Engineering Research (IJATER), 7(6), 36–41.

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. IEEE/CVF CVPR, 815–823.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Online ISSN 3007-3197
Print ISSN 3007-3189

Sharma, N., Kumar, V., & Singla, S. K. (2021). Single Image Defogging Using Deep Learning Techniques: Past, Present and Future. Archives of Computational Methods in Engineering, 28, 4449–4469.

Sharma, V., & Kumar, M. (2025). Improving intrusion detection with hybrid deep learning models: A study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. Journal of Information Systems Engineering and Management, 10(11S), 633-650.

Suganya, R., & Kanagavalli, R. (2020). On the Review of Dehazing Methods for Bad Weather Images. IJETT, Special Issues ICT 2020, 90–98.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Vidal Filho, et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International journal of machine learning and cybernetics, 14(2), 513-535.

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Online ISSN 3007-3197
Print ISSN 3007-3189

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland.

Zhu, Q., Mai, J., & Shao, L. (2015). A Fast Single Image Haze Removal Algorithm Using Color Attenuation Prior. IEEE TIP, 24(11), 3522–3533.

Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: A survey. Information Systems Frontiers, 17(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7