International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Investigations Oncloud, Wireless Networking And Block Chain For High Encrypted Communications - A Detailed Survey

G.Shangkavi[1], S. Sarveswaran[2], Naveenbalaji Gowthaman[3], S. Vasanthaseelan[4]

[1]Electronics and Instrumentation Engg.,Sri Ramakrishna Engineering College,Coimbatore,641022, India.
[2]Robotics and Automation, Sri Ramakrishna Engineering College, Coimbatore,641022, India.
[3]Electronic Engineering, University of KwaZulu-Natal, Durban,4041, SouthAfrica.
[4]Assistant Professor (Sr. G), Mechanical Engineering, KPR Institute of Engineering and Technology, Coimbatore, 641407, India.

Email :[2]sarveswaran10@gmail.com

Abstract.The easy usage of cell phones, IoT (Internet of Things), social media, analytics, and cloud technology that develop models for smarter decisions has provided the digital world new inventive goods, efficiencies, and fantastic consumer interactions all around the world. In this paper, Certain investigations on Cloud, Wireless Networking and Block Chain Technology for high encrypted communications are surveyed. In case of cloud, generic secure data storage model, A randomized client-side deduplication scheme, Bayesian Attack Graphs, cloud data deduplication scheme is been discussed along with its performance. And encryption techniques include GROSE approach, MCBE Scheme in the public key setting, dynamic Boolean SSE Scheme is discussed. In wireless networking, cluster-related routing protocol for WSNs, a dynamic spectrum access scheme, Mixed Integer Programming (MIP), In WMSN approaches, energy-efficient distributed adaptive cooperative routing is discussed. Bloch chain technologies like DV – PoA (designated – verifier proof of assets) and other networks likeVehicular and hoc networks – (HMAC), FASUS mechanism, PV/WEC Particle Swarm Optimization algorithm, SimpleStab, Online supervised method, UIPA, DNN algorithm, Snort and Suricata and finally USM sharpening detection algorithm for JPEG image performances are surveyed.

Keywords: Internet of Things, Multi-Channel Broadcast Encryption, Searchable Symmetric Encryption, Wireless Sensor Networks, Mixed Integer Programming.

1. INTRODUCTION

The demand for computer system resources, notably data storage (cloud storage) and computational power, without direct active control by the user is known as cloud computing.The term refers to data centres that are accessible to a huge number of people over the Internet. In huge clouds, functions from central servers will be spread across many different places.If the connection to the user is close, it may be classified as an edge server. Clouds can be used by a single company (enterprise clouds) or by a group of companies (public clouds). Cloud computing makes it easier to share resources and maintain consistency.

Cloud computing enables businesses or industries to plan ahead and save infrastructure expenditures. They also claim that cloud computing enables business applications to run faster, with greater manageability and less maintenance, and that it enables IT teams to obtain resources to meet fluctuating demand, resulting in the blast computing capability, which provides high computing power at peak demand.Cloud providers operate under a "pay-as-you-go" paradigm, which might result in significant running costs. The rise of cloud computing is due to the availability of resources such as high-capacity networks, low-cost processors, and storage devices, as well as the broad adoption of hardware virtualization, service-related architecture and acting, and utility computing.In 2017, the majority of cloud machines used a Linux-based operating system.

Wireless connections between network nodes are used in a wireless network.Wireless networking, telecommunications networks, households, and business installations eliminate cables and replace them with wireless connections.Radio communication is commonly used to execute and operate admin telecommunications networks.At the OSI model's physical level, this implementation occurs (layer).Wireless sensor networks, satellite communication networks, mobile phone networks, wireless local area networks (WLANs), and terrestrial microwave networks are all instances of wireless networks.

Cryptography is used to connect blockchains. A cryptographic hash of the preceding block, a timestamp, and transaction data are all included in each block (generally represented as a Merkle tree). The timestamp shows that the transaction data was valid at the time the block was published, allowing it to be hashed.Because each block carries information about the one before it, they create a chain, with subsequent blocks reinforcing the ones before them.As a result, blockchains are resistant to data changes since the contents in any block, once recorded, cannot be modified without impacting all subsequent blocks.

Encryption is the process of encoding data in cryptography.This method transforms plaintext data into ciphertextdata.Only an authorised person may successfully convert ciphertext to plaintext and gain access to the original data.Encryption does not prevent noise from other signals, but it does deny a would-be interceptor access to plainly intelligible material.

An encryption scheme must always utilise a pseudo-random encryption key technique for technical reasons.It is simple to decode the message without knowing the key, but expensive computational resources and abilities are required for an encryption system.With the key provided by the originator to receivers, an authorised individual can easily decrypt the communication, but not unauthorised users.

Historically, various encryption isused to help in cryptography. Early encryption techniques were highly used for military messaging. Andlater, new techniques have developed and became common in every aspects of modern computing. Modern encryption schemes utilize the public-key and symmetric-key concepts. Modern encryption techniques make sure security because modern computers are not efficient at cracking the encryption.

2. FOUNDATIONAL CLOUD COMPUTING TRENDS

Cloud computing was shaped by technological advancements as well as an increase in services.The following are some of the most significant developments.

1. Containers

Containers are used in a variety of settings.Packaged software and operating systems are what they are.The applications contain dependencies and binaries that isolatethe host operating system's activities.

Containers are critical to the growth of cloud services and as a foundation for the development of cloud-native applications.Many firms' production environments are going to employ containers, according to Forrester.

Containers are widely used because they assist organisations and ensure that data can be readily transferred between cloud services.As a result, DevOps methodologies are supported, resulting in teams and products that are more productive.

2. Serverless Computing

On managed infrastructure, serverless computing takes place.It relieves IT and DevOps teams of back-end responsibilities,allowing engineers to concentrate on the functionality of the application or code.Azure Functions, AWS Step Functions, and Google Cloud Functions are some instances of serverless services.

Serverless computing allows companies of all sizes to access resources without incurring any upfront fees or hardware investments.This appeals to businesses because it allows them to experiment with resources and code before making large commitments.

3. Cloud Security

As the popularity of cloud services expanded, so did the risks to data and applications housed in the cloud. This has accelerated the growth of cloud-based security and data privacy.

Cloud security has supported cloud service expansion in a variety of ways. Enterprise-grade security measures will be included in the services of major cloud providers.Cloud-based security solutions have evolved to protect data both on-premises and in the cloud.

In addition, managed cloud security services are becoming increasingly popular.These are third-party services that monitor a company's assets for security.

4. Edge Computing

Due to the distributed nature of cloud resources, latency and accessibility needs have changed dramatically.The number of users and data shared among cloud services have to keep increasing.This spread has been aided by edge computing, which brings data analytics and computation operations closer to people and devices.

As the Internet of Things (IoT)andbig data become increasingly common, edge computing is becoming more significant.Real-time data analysis and artificial intelligence application improvements can benefit from this form of computing.This could make cloud services even more accessible and advantageous to organisations who have been hampered by latency in the past.

5. Managed Open-Source Services

Open-source deployments can be outsourced to public cloud hosting providers such as AWS, GCP, Azure, and others by managed open-source service providers.

Managed service providers not only host but also maintain the services, providing features such as automatic version upgrades, data replication, and so on.

Using a managed service allows you to concentrate on data and applications rather than the underlying infrastructure. Open-source deployments benefit from managed services' durability

and stability, as well as the ability to create performance data pipelines in minutes with minimal maintenance issues.

6. High-Performance Computing (HPC)
Supercomputers, which were previously only available to huge enterprises, organisations, or governments, were required for large computations or data processing operations. Due to the cloud, Supercomputer infrastructure is becoming increasingly available to all organizations.
HPC instances, which are highly parallelized and offer massive computing capabilities at a modest cost, are available from all major cloud providers. These HPC cloud services are used by businesses for compute-intensive processes such as genomics, risk management, and big data analysis.

3. EVOLUTION OF BLOCKCHAIN: PHASE 1- TRANSACTIONS

2008-2013: Blockchain 1.0: Bitcoin Emergence
Many individuals believe that Bitcoin and Blockchain are interchangeable terms.This is not the case, as cryptocurrencies are the technology that underpins the majority of applications.
Bitcoin, which was released in 2008, was theBlockchain technology's initial application.In his whitepaper, Satoshi Nakamotocharacterised it as an electronic peer-to-peer system.The genesis block was created by Nakamoto, and it was used to mine subsequent blocks, As a result, one of the greatest chains of blocks carrying various bits of data and transactions has emerged.
Many apps have sprung up since Bitcoin, a blockchain application, hit the airwaves, all of which seek to utilise the ideas and capabilities of blockchain.

4. EVOLUTION OF BLOCKCHAIN: PHASE 2- CONTRACTS

2013-2015: Blockchain 2.0: Ethereum Development
As one of the initial contributors to the Bitcoin source, VitalikButerin is one of a growing number of engineers who believe Bitcoin has yet to fully leverage the powers of blockchain technology.
Concerned about Bitcoin's limits, Buterin began developing a customizable blockchain that can serve a variety of activities in addition to acting as a peer-to-peer network.Ethereum, a new public blockchain with more functionality than Bitcoin, was introduced in 2013, marking a watershed moment in Blockchain history.
Buterin created Ethereum unique from BitcoinBlockchain by including a feature that allows users to store assets other than bitcoins.
Since its official launch in 2015, Ethereumblockchain has grown to become one of the most popular blockchain applications due to its capacity to handle smart contracts that can perform a variety of tasks. The Ethereumblockchain platform has also attracted a thriving developer community, resulting in the development of a true ecosystem.
On a daily basis, the Ethereum blockchain processes the most transactions.The market capitalization of cryptocurrencies has also risen dramatically.

5. EVOLUTION OF BLOCKCHAIN: PHASE 3- APPLICATIONS

2018: Blockchain 3.0: the Future
Ethereum and Bitcoin are just the beginning of the blockchain'sevolution.A increasing number of projects have arisen in recent years that all employ blockchaintechnology.While incorporating new blockchain-based functionality, new projects have attempted to remedy some of Bitcoin and Ethereum's flaws.
One of the most recent blockchainapplications is NEO, China's first open-source, decentralised, and blockchain platform. Despite its ban on cryptocurrencies, the government remains a pioneer in blockchain technology. NEO positions itself as the Chinese Ethereum, with Alibaba CEO Jack Ma already endorsing it as it aspires to have the same impact as Baidu in the country.
IOTA was founded in the race to use blockchain technology to accelerate the development of the Internet of Things. The cryptocurrency platform aims to provide zero transaction fees and innovative verification mechanisms, making it ideal for the Internet of Things ecosystem.Along with Blockchain 1.0 Bitcoin, it also tackles some of the scalability difficulties.
Other second-generation blockchain systems, in addition to IOTA and NEO, are causing a ripple effect in the industry.TheblockchainsMoneroZcash and Dash were created to overcome some of the security and scalability difficulties that plagued early blockchainapplications.The three blockchain platforms, dubbed privacy Altcoins, promise high levels of privacy and security in terms of transactions.
The above-mentioned blockchain progression involves public blockchain networks, in which anybody can view the contents of a network. However, as technology has advanced, a growing number of businesses have begun to utilise it in order to improve operational efficiency.
Large firms are investing heavily on expert recruitment in order to obtain a head start on technology adoption. Companies like Microsoft and Microsoft have led the way in creating blockchain technology applications, resulting in what are now known as private, hybrid, and federated blockchains.
2015: Hyperledger

The Linux Foundation launched the Umbrella open-source blockchain project in 2015.They named it Hyperledger, and it has since served as a collaborative development platform for distributed ledgers. Hyperledger aspires to foster cross-industry collaboration for the development of blockchain and distributed ledgers under the leadership of Brian Behlendorf.
Hyperledger is a non-profit organisation dedicated to promoting the use of blockchain technology to improve the performance and stability of modern business systems around the world.

2017: EOS.IO
EOS is based on the concept of a private business block. One was formed in 2017, when a new blockchain system with EOS as its native token was released.EOS, unlike other blockchain protocols, aims to increase real-world computer functions such as CPU and GPU.
As a result, EOS.IO serves as a decentralised operating system as well as a smart contract platform.Its primary goal is to promote the usage of decentralised apps by forming a self-

contained decentralised organisation.

To offer an intelligent transportation system, the interchange of information between vehicles and between vehicles and infrastructure through vehicular ad hoc networks (VANET) should be secured and protected.For security, VANET relies on certificate revocation lists (CRL) and public key infrastructures (PKI).PKI algorithms examine the sender's certificate in the current CRL, as well as the authenticity of the sender's signature and certificate, to ensure that communications received from the sender are valid.Checking the CRL and validating its authenticity takes time and slows down the system. This paper provides a faster and safer authentication solution for revocation checking that uses a hash message authentication code (HMAC) in conjunction with secret keys. By using HMAC and enhancing the CRL checking mechanism, the strategy improves system metrics including end-to-end delay, authentication delay, and packet delivery ratio [1].

Numerical data produced from NS-2 simulations for an intelligent vehicular system in random city situations with varied vehicle density and for different keys sizes of 128, 192, and 256 bits are used to evaluate the proposed algorithm's performance.By observing that key size modification has no substantial impact on the system's performance [1].

Fast association in 802.11ah networks aims to quickly associate a large number of units with an access point. Fast association mechanisms now in use have efficiency, fairness, and robustness issues.They propose the FASUS (Fast Association based on Speculating the number of Stations) technique in this research.FASUS implements innovative retransmission, thresholding, and adaptive round selection methods, significantly improving association performance.When compared to one of the most well-known processes for 802.11ah networks, the Linear Increase Linear Decrease (LILD) approach, experiments demonstrate that FASUS will shorten the association time by 67.1 percent. They develop a mathematical model to investigate the association process and determine the optimal number of stations every round. In congested networks, they also propose two ways for dealing with inter- and intra-network interference. The propose of new ways to combat two assaults in order to increase the network's robustness and fairness: 1) a denial-of-service (DoS) assault that can bring the entire network down, and 2) a selfish node attack that allows attackers to connect considerably faster than normal stations [2].

FASUS outperforms known mechanisms such as LILD, MM, CAC, and DOWN by a large margin.The proposed technique cannot assure fairness if the MAC address is changed by the user to facilitate a quick association [2].

Cloud computing is the most effective technology for delivering and managing resources on a pay-per-use basis.Generally, various organizations stockpile documents in a group.The current methods use encryption algorithms to secure the values in the documents.However, these algorithms take a long time to encrypt and demand additional storage space. It takes a long time to apply encryption techniques, and they don't require any security.However, the sensitive information in these documents varies from one user to the next, and this sensitive information, too, must be protected.A generic safe data storage approach is developed to address these challenges.The suggested cloud-based generic secure data storage approach requires less encryption time and space [3].

CSS's key concerns include security and privacy, as well as storage costs.The suggested project was for a text document storage system based on templates.This sensitive data is subjected to the EECC method.The sensitive properties are grouped into ‘n + 1' groups to improve security.When compared to the existing technique, the suggested system requires significantly less storage space, resulting in lower computing costs [3].

In BroadcastProxy Re-encryption, the GROSE algorithm is presented to determine the best receiver group size.The Rubinstein–Sthl bargaining method is used by GROSE.The sender and receiver benefit from each other, and the overall reward rises. Proxy re-encryption is a critical step in securely transmitting data from the cloud to another user.The broadcast proxy re-encryption feature was added to enable for safe data exchange across several users.However, if the receivergroup is large, and the receivers in the group must calculate the additional costly algebraic operations, the receiver will incur an overhead.They approach the problem from the perspective of a bargaining game, the Rubinstein–Sthl bargaining game.Finally, they put GROSE into practise and compare it to the preceding systems.According to the findings, GROSE outperforms classic proxy re-encryption and broadcast proxy re-encryption techniques [4].

When opposed to employing the Broadcast PR, each receiver's decryption cost is lowered.As a result, GROSE's total payout is much higher than both the TPR and BPR schemes' total payouts. The GROSE technique is still under development, with the sender's encryption key generation cost being less than the Broadcast PR and each receiver's decryption cost being less than the standard PR [4].

The goal of this project is to analyse, design, and construct a DC/DC buck–boost converter for the production of a hybrid prototype using a wind energy conversion system with 3kW PV and 3.2 kW PMSG.The Particle Swarm Optimization approach is used to regulate the output voltage generated.The PSO approach is used to extract maximum power from NP-hard situations such as hybrid renewable energy sources. To reduce harmonics and supply maximum electrical output to the grid on polynomial time, a single phase or three phase sinusoidal pulse width modulation (SPWM) inverter was used with a PQ control technique based on metaheuristics. Using an LC filter, the proposed PSO approach generates a steady state DC connection voltage of 400 V with reduced harmonic distortion.Additionally, the use of a capacitor bank lowers output voltage change ripples. The simulation results demonstrate that the proposed model is accurate in its measurements [5].

The suggested hybrid PV/WEC system fed buck–boost converter can be used in a variety of applications.The solar module provides roughly 5 kW of maximum electricity from the PV module. WECS, on the other hand, generates a maximum of 4.2 kW of power at a wind speed of 13 m/s and a tip speed ratio of 8.1. This proposed model performs well in the event of a sudden change in weather conditions. The harmonic distortion is 1.68 percent and is reduced to 0.57 percent when PSO uses the metaheuristic condition.Dead beat PQ control strategy Using output voltage regulation, the SPWM control technique regulates and maintains the DC link output voltage constant at 470 V [5].

Cluster Heads (CHs) in a Wireless Sensor Network (WSN) transmit more traffic than regular sensor nodes. Because they aggregate data from all of the sensor nodes in their cluster before transmitting it to the sink, or base station, they are able to do so. The Load Balanced Clustering Problem is the task of minimising the load on the CHs (LBCP).This paper proposes a cluster-based routing strategy for WSNs. It solves the LBCP's fpt-approximation algorithm, which has an approximation factor of 1.1 and a running time of 2O(dmax/ log(dmax) + O(n), which makes it much clearer than previous approximation factors.Because the running time of dmax is merely exponential, it's perfect for large-scale WSNs.To discover the best routing tree that connects the CHs to the sink, the proposed protocol employs an energy-aware routing method. The routing algorithm selects specific channels for delivering data to the sink and changes them at specific intervals to balance node energy consumption and maximise network

lifetime. The simulation findings imply that the suggested protocol performs better than other similar protocols.They recommend two study topics for the future.The first goal is to reduce the amount of time it takes to run the suggested fpt-approximation algorithm.The second task is to create an identical fpt-algorithm for LBCP that includes the parameter defined in this study [6].

Client-side deduplication is commonly utilised in commercial cloud services to conserve server resources.This type of deduplication technique, on the other hand, is prone to collusive authentication, brute-force attacks, and duplicate-faking attacks. The majority of current techniques fail to address these problems.Furthermore, how to implement ownership management in client-side deduplication to maintain forward and backward data confidentiality is a hot subject right now. They describe a randomised client-side deduplication technique in this work, which employs a randomised deduplication procedure to prevent collusive authentication and offline brute-force attacks, as well as storing data according to two file tags to prevent duplicate-faking attacks. They also use a dynamic Key-Encrypting Key tree to offer more accessible ownership management and data transmission. The suggested technique may meet the specified security criteria while saving system resources efficiently, according to security and performance study [7].

To improve cloud services while lowering server load, they devised a novel data sharing mechanism based on a dynamic KEK tree. The proposed scheme satisfies the required security standards. As a result, both the theoretical analysis and the visualised simulation result show that the proposed strategy is quite effective [7].

Many videos have appeared on professional video websites in the recent decade as a result of the increasing rise of edge devices such as mobile phones, and they are easy to retrieve. The bulk of movies made by smartphone cameras, on the other hand, are unstable and even motion blurred. The user experience may be harmed by these low-quality videos.As a result, the challenge of removing jittery difficulties and making unstable films stable is critical.They offer a novel method for video stabilisation in this paper to improve the stability of low-quality footage. SimpleStab is the proposed method, which incorporates motion estimation, trajectory smoothing, and image compositing.Because of its unique architecture, TheSimpleStab can not only analyse offline videos but also live video streaming. They conducted a thorough experiment on the benchmarking dataset and compared their results to current methods.According to experimental results, SimpleStab outperforms state-of-the-art techniques [8]

As we all know, unstable video sequences have a huge impact on augmented reality (AR) applications.The AR system, on the other hand, necessitates not only a computationally inexpensive video stabilisation approach, but also the required precision. There has never been a rapid video stabilisation technology. To solve these problems, SimpleStab is proposed, which has both quick speed and high accuracy and achieves the best balance between computational cost and precision. SimpleStabis' sparse feature trajectory correction requires no sophisticated computation and is ideally suited to mobile devices. When evaluated on publicly accessible benchmarking datasets, the SimpleStab technique outperforms the state-of-the-art method.In addition, the SimpleStab has been integrated effectively into an AR system. Finally, for the AR application, a precise, quick, and effective video stabilisation solution is provided. Three-dimensional reconstruction based on live video streaming will be included in future versions of the SimpleStab [8].

Multi-channel broadcast encryption (MCBE) is a modern digital technological method that provides various messages to separate groups of users in real-world applications such as TV

broadcasts, radio broadcasts, and so on.This work [9] proposes two multi-channel broadcast encryption techniques in the public key context, the first of which focuses on selective security against plain text attacks and the second of which achieves adaptive security in the broadcast setting.Furthermore, the second structure has a dynamic aspect that allows the broadcaster to lower the cost of encryption and decryption by picking the lowest set of subscribers and revoked in both stages.[9]

As a contemporary of technologies with vast applications ranging from finance to social services, blockchain has gotten a lot of attention from a variety of domains.Since the growth of blockchain technology in e-commerce services, crypto currencies have grown in popularity.Some currencies, such as bitcoin and ethereum, have taken use of blockchain'sdecentralisedstructure.Becauseblockchain is a distributed database system, it can be attacked by bad users, hence it must rely on encryption for security. On this article[10], the authors explore numerous features of blockchain, including its taxonomy and focus on blockchain structure, as well as the workings of current transactions in the bitcoin network. This essay also looks into the taxonomy of blockchain and its features, as well as real-world applications and a full comparison based analysis with existing security issues under challenges chain knowledge systems.Several new features of Bitcoin and Ethereum are described, and the author outlines recent advancements in the realm of blockchain technology that could be used to deploy and develop the Bitcoin and Ethereum networks.[10]

This paper [11] provides a novel online self-supervised approach for learning face identities in unconstrained video streams based on face appearance collectively. Deep facial feature descriptors are combined with a memory-based learning mechanism that takes advantage of the temporal coherence of visual input in this one-of-a-kind technique. They also talked about how to apply MOCAL (Multiple Object Cumulative Adaptation Learning), Multiple Object Tracking, and Continual Learning to vi, as well as a discriminative descriptor matching solution based on Reverse Nearest Neighbor and a memory-based cumulative learning strategy that eliminates redundant descriptors.

This methodology[11] allows for the collection and preservation of vital knowledge while simultaneously dealing with data stream non-stationarity.According to experimental data,The proposed technique is theoretically sound, asymptotically stable, and can be implemented in real time.In comparison to Multiple Object Tracking techniques, the method's effectiveness has been demonstrated over public datasets.The technique is also shown to be capable of effective cumulative learning across long, unrestricted video sequences. As a result, with the availability of detector/feature combinations, this method can theoretically be used to any other setting, such as a vehicle, person, boat, or traffic sign.[11]

The World Wide Web (WWWW), often regarded as one of the greatest computer technologies, has revolutionised the way humans communicate and share information. One of the most common problems that users have in the online world is user authentication, and the majority of users find it difficult to remember some of the strong passwords.The User Interface Preference Authentication, as proposed in this work [28], is a novel authentication technique strategy based on user interface (UI) preferences (UIPA).Depending on the experimental results, this user interface (UI) makes password recovery easier based on his or her particular qualities.The false positive rate for UIPA is at 0.416 percent, whereas the false negative rate is around 0% [12].

The total performance of the UIPA approach was measured in this research using a two-stage experiment, and the results are highly promising.TAM has also been used to determine user

approval of the UIPA approach. As a result of the findings, people have expressed an interest in using this technology as a password recovery alternative.One of the most significant benefits is that the user is not obliged to recall specific information and instead has the ability to select choices based on their personal traits. One of the method's significant drawbacks is that the tests are only available to those who use desktop computers/laptops and do not take into account smart gadgets or smartphones. To summarise, as compared to the present ways of account recovery, UIPA can be used as an effective and efficient method.[12]

When it comes to cloud service provisioning, virtualization security is a critical consideration.They offer the Bayesian Attack Graphs (BAG) model for evaluating security risk for platform virtualized infrastructures, which are used in this study to provide cloud services. BAGs can be used to mimic the unpredictability of security threats. They use reported attacks on virtualized systems from the Common Vulnerabilities and Exposures (CVE) database to create conditional probability tables for the BAG nodes. They use Bayesian probabilistic inference techniques on the model supplied and show the results, which system builders can use to predict the risk of such infrastructures. They propose a deterministic approach with security metrics for attack graphs and generate values for the modelled BAG, which can be used for analysis and comparison with other systems, in addition to the probabilistic model. System architects can use the approach provided here to draw conclusions from the BAG in order to find answers to crucial questions in security design, as well as to select countermeasures with caution. The model can also be utilised to give an efficient risk assessment by learning from future a-posteriori evidence data from actual security breaches [13].

System administrators and architects of virtualized infrastructures can utilise the model presented here as a basic reference model for planning and evaluating security problems. By integrating countermeasures at various stages, the model may also be used to generate alternative conditional probability assignments and evaluate their success in reducing the risk associated with the overall infrastructure [13].

The current research efforts on wireless communication systems of the Fifth Generation (5G) have revealed the need for significant improvements in communication service accessibility and reliability.In this regard, Cognitive Radio (CR) has been envisioned as a major 5G enabler that allows for dynamic spectrum access while simultaneously addressing the issue of ultra-reliable communication without interfering with licenced (primary) users. Channel failures, which are caused by hardware and software faults as a result of built-in features like fading and shadowing, can significantly degrade network performance. The connections of unlicensed (secondary) users in cognitive radio networks (CRNs) are naturally vulnerable to breaking owing to channel faults and the arrival of licenced users. They propose and evaluate the benefits of channel reservation and retrial phenomena on performance enhancement in error-prone channels using a dynamic spectrum access (DSA) system that considers baulking and reneging behaviour.In addition, because 5G networks are likely to include a diverse set of apps with various Quality of Service (QoS), the current study advocates the use of heterogeneous secondary users with varying access privileges. Furthermore, while much previous research has concentrated on CRNs' stationary performance, this may not be enough in practise, especially when operations have a finite time horizon. Using dependability theory as a lens, this study examines transient dynamics in CRNs.A multi-dimensional continuous time Markov chain (CTMC) is used to describe the entire system, and numerical results suggest that the proposed technique has the potential to considerably improve the error-prone

CRNs performance [14].

Despite major research efforts over the last decade, nothing is known about the transient analysis of CRNs from the perspective of dependability theory.This paper proposes a dynamic spectrum access solution with channel reservation and a retry mechanism. Theuniformization tool is used to create mathematical formulations for channel access transient performance measurements in CRNs.The proposed strategy's performance was assessed using CTMC modelling.Contrary to common assumption, channel reservation does not always provide suitable performance trade-offs; rather, its success is primarily reliant on the network's condition.

Despite the fact that channel reservation may not be required at very short time intervals or with very low channel failure rates, the suggested reservation strategy is recommended for QoSprovisioning. Furthermore, the rate of channel failure and recovery has a substantial impact on the availability and reliability of end-user services. Furthermore, the data suggest that using the retry phenomenon, which is vulnerable to baulking and reneging, improves CRN performance by increasing SU performance. The scheme described in this study, we believe, provides a systematic approach for analysing time-dependent channel access reliability in multichannel CRNs [14].

Popular programmes for sharing data, such as text, photographs, and videos, are known as Online Social Networks (OSN).Fake account issues, on the other hand, are a major roadblock in the existing OSN systems. To transmit fraudulent information such as malware, viruses, and dangerous URLs, the attacker creates phoney accounts. DeepProfile, a DNN solution for dealing with false account difficulties, is based on deep learning's significant breakthroughs in computer vision, automatic feature extraction, and representation. Instead of utilising traditional machine learning, they used a dynamic CNN to train a false profile categorization learning model. They present a novel pooling layer to increase neural network training performance, which is very impressive. Experiments show that they perform well in a malicious account categorization test [15], with higher accuracy and lower loss than traditional learning methods.

To deal with the difference from what is typical, several ways provide statistical methodology and learning algorithms combined with human feature engineering.Feature engineering and computational resources, on the other hand, are expensive. They develop DeepProfile, a model that deals with erroneous profile categorization by using a novel CNN with a generic pooling function instead of traditional learning. The WalkPool pooling layer is used to create a dynamic CNN architecture that optimises CNN computation and improves accuracy.They used gradient descent techniques to train CNN in the experiment, altering the learning rate (lr = 0.01) to compute the stride size in order to attain a (local) minimum. They discover that the SGD with momentum (momentum = 0.8) can produce a competitive outcome by displaying the classifier with specific hidden layers. Using the SGD with momentum, the suggested CNN to conduct the classification for detecting phoney profiles is better trained and tested. In this scenario, it outperforms the dynamic optimizers Adam, Adagrad, and RMSProp in terms of accuracy and loss.They construct the AUC and ROC curve as an evaluation metric to measure the classifier's performance in addition to the accuracy and loss. The network harvests the maximum percentage of the region within the ROC score in the range0.9500~0.9590, according to the ROC. Because it provides AUC = 0.9547 and exceeds other traditional learning algorithms, the DeepProfile achieves good level predictions.They acquire higher accuracy and lower loss than traditional learning algorithms by demonstrating the DeepProfile with the WalkPoolpooling function. It's also a good method for teaching a CNN model to

solve a classification challenge. The pooling function can be utilised to produce a good result and faster speed in a large dataset like OSN.Implementing the Deep-Profile network with WalkPool function significantly improves the speed of the CNN graph.Finally, rather than relying on node information, future study could focus on a semantic network structure feature to anticipate an OSN's anomalous node. In the future, it will be necessary to investigate how to handle account and virus hierarchy links.The threat's source is reflected in the hierarchy.Then, rather than using an ordinary loss function, a novel technique called adaptive loss function must be used to calculate neural network computation. It is also required to design a novel network training regulator in order to achieve an efficient result [15].

For the first time, bitcoin is based on the blockchain's basic technique.Bitcoin is a payment method and a digital money. The bitcoin exchange uses the blockchain to safeguard the anonymity of its customers. In some circumstances, demonstrating the buyer's asset strength is necessary in order to avoid troublemakers. At the same time, the buyer's assets must be kept private.In this work, they present the novel DV-PoA (designated-verifier proof of assets) concept for bitcoin exchange. They created the first actual DV-PoA system that uses elliptic curve encryption to be consistent with the bitcoin exchange's signature, which also uses elliptic curve cryptography. They then demonstrate the suggested DV-PoA scheme's security.Then, using the two scenarios of theory and practise, they assess its efficacy.According to their findings, the developed DV-PoA strategy is both secure and efficient [16].

There are certain significant difficulties in the DV-PoA research sector that have yet to be solved.They will investigate the following issues in the future.When a buyer or a seller is made up of multiple entities, a safe multi-part calculation on the blockchain is required.What is the most efficient method for constructing a multi-party DV-PoAscheme using a multi-party calculation? The hash value of the public key is the address in the public blockchain. The privacy of the public key can be protected by a ring signature. How can ring signature be used to keep the public key private in DV-PoA when the address is public and the public key is hidden in the hash function? They use elliptic curve cryptography to create a novel notion of designated verifier proof of assets for bitcoin exchanges in this paper. They provide a formal definition, system model, and security model for the novel security primitive. They then construct a concrete DV-PoAstrategy utilising elliptic curve cryptography. After investigating the security and performance of their developed DV-PoA approach, they found it to be provably secure and efficient [16].

With the advancement of information technology, the amount of created user data has expanded dramatically, posing an issue in which the server is overburdened with comparable data. In this paper, the author described a cloud data deduplication approach that allows redundant data blocks or files to be removed from the cloud storage server and only one copy to be stored.To detect a ciphertext and locate identical files, the certificateless proxy re-encryption (CL-PRE) and proof of ownership based on certificateless signature (PoW-CLS) techniques are utilised. To solve the key escrow problem, the author proposes certificateless cryptography, which prevents the key generation centre (KGC) from impersonating a user when decrypting the ciphertext.CL-PRE makes data deduplication easier for consumers, while PoW-CLS makes proof of ownership more efficient (PoW). [17] SSE is utilised in a variety of industries where a collection of encrypted documents must be outsourced to a remote server and keyword searches on these encrypted documents must be performed with the server knowing as little as possible.In the random oracle situation, several contemporary SSE algorithms are only adaptively secure against the untrusted server.As a result, when

constructing an SSE scheme, it is necessary to examine the security of the standard model. The authors of this paper[18] provide a dynamic boolean SSE technique in a multi-client setting that uses BE to eliminate per-query interaction between the data owner and the client, leading in a considerable reduction in query time.

Table 1
Advantages and Disadvantages of Certain Investigations on Cloud, Wireless Networking and Block Chain Technology for High Encrypted Communications

Reference	Method	Advantage	Disadvantage
[1]	vehicular ad hoc networks - hash message authentication code (HMAC)	algorithm provides improved performance of the system	
[2]	Fast Association based on Speculating the number of Stations (FASUS) mechanism.	considerably increase the performance of the association. They suggest novel ideas to increase the network's robustness and fairness.	Existing quick association mechanisms have inefficiencies, inequity, and robustness. If the MAC address is altered by the user to accommodate a rapid association, the proposed approach cannot ensure the fairness.
[3]	generic secure data storage modelfor cloud	takes lesser encryption time and storage space	
[4]	GROSE - Rubinstein–Ståhl bargaining approach	Traditional proxy re-encryption and broadcast proxy re-encryption techniques are less efficient than GROSE.	
[5]	hybrid PV/WEC system fed buck–boost converter, Particle Swarm Optimization algorithm	The proposed model works well in the event of a sudden shift in climatic circumstances.	
[6]	a WSN routing protocol based on clusters	In comparison to previous similar protocols, the proposed protocol performs better.	
[7]	A randomized client-	The proposed approach may	

	side deduplication scheme	meet the specified security requirements while saving system resources and providing outstanding performance, according to security and performance studies.	
[8]	SimpleStab	SimpleStab is the proposed method, which is fast and accurate, and provides the best balance between computational cost and accuracy.	
[9]	In the public key situation, there are two multi-channel broadcast encryption schemes.	highly deals with selective security against plain text attack and achieve adaptive security in broadcast setting.	
[10]	blockchain	the advancements in blockchain technology that could be used to deploy, improving the Bitcoin and Ethereum networks	
[11]	online self-supervised method	The proposed strategy is theoretically sound, asymptotically stable, and works in the real world.	
[12]	User Interface Preference Authentication (UIPA)	One of the most significant benefits is that the user is not needed to recall specific information and instead has the ability to select choices based on his or her own traits.	A major limitations of this method is that the experiments are available only to the uses who used desktop computers/laptops and did not consider smart devices and smartphones.
[13]	Bayesian Attack Graphs	The model can also be used to create security frameworks by integrating countermeasures at different phases to provide alternative conditional probability assignments, allowing you to assess their effectiveness in lowering	

		total risk..	
[14]	a channel reservation and retrial policy for a dynamic spectrum access system	Using the retry phenomenon, which is prone to balking and reneging, has a major impact on CRN performance by enhancing SU performance.In multichannel CRNs, It also offers a method for studying the time-dependent reliability of channel access.	
[15]	DeepProfile, a deep neural network (DNN) algorithm	a promising result with increased precision Because it provides AUC = 0.9547 and exceeds other traditional learning algorithms, the DeepProfile achieves good level predictions. The performance of the CNN graph has significantly improved.	Adam, Adagrad, and RMSProp all have lower losses than the dynamic optimizer.
[16]	DV-PoA (designated-verifier proof of assets)	The DV-PoA technique has been proven to be both secure and efficient.	There are several challenging issues that have yet to be resolved.
[17]	cloud data deduplication scheme	CL-PRE facilitates data deduplication among users, whereas PoW-CLS improves the efficiency of proof of ownership (PoW)	
[18]	dynamic boolean SSE scheme	In the standard model, the proposed approach achieves provable security against the adaptive adversarial server and malicious clients, and the performance research demonstrates that the findings are promising for a wide range of applications.	
[19]	Mixed Integer Programming (MIP)	Binary Compressive Sensing (BCS) and Indoor Solar Harvesters (ISH) considerably extend the life	

		of industrial networks.	
[20]	Snort and Suricata	Performance benchmarks in 100 Gb/s networks to better understand drop rates and detection accuracy.	
[21]	WMSN distributed adaptive cooperative routing that is energy-efficient	Energy usage is lowered while maintaining QoS when compared to traditional protocols.	
[22]	For JPEG images, an efficient USM sharpening detection technique is used.	superiority of the suggested approach in detecting sharpening in small-size photos over the present method.	

communication overhead.Furthermore, the paper provides a new effective T-set instantiation from a clear storage system that supports index file update by constraining the ciphertext length in BE to a constant. In the standard model, the proposed technique achieves provable security against the adaptive adversarial server and malicious clients, and performance study shows that the findings are promising for a wide range of applications.

[18]

Wireless multimedia sensor networks (WMSNs) have grown in popularity in industrial applications due to their wide variety of applications and low cost.The enormous data size of WMSNs is one of their main problems, which leads to greater energy consumption during transmission, posing a serious challenge for the network's longevity.The major goal of this paper[19] is to see how data compression and Compressive Sensing (CS), as well as EH techniques like vibration, thermal, and indoor solar, affect the longevity of WMSNs in industrial settings. When EH, CS, and Error Control (EC) approaches are used together, this research [19] provides a new Mixed Integer Programming (MIP) framework to maximise network longevity. According to comparative performance studies, using Binary Compressive Sensing (BCS) and Indoor Solar Harvester (ISH) considerably extends the lifetime of an industrial network[19].

Intrusion Detection Systems (IDSs) have long been used to detect malicious activity in a network. Industry and academic organisations are establishing 100 Gb/s networks to meet expanding data transfer needs, but this activity has created substantial technological problems. When monitoring enormous and diversified traffic volumes, an Intrusion Detection System (IDS) cannot process network activity at such a fast rate, resulting in a high packet drop rate, which has a major influence on detection accuracy. The authors of this paper[20] investigated two prominent open-source IDSs: Snort and Suricata, as well as their performance benchmarks, in order to gain a better knowledge of drop rates and detection accuracy over 100 Gb/s networks. The study examines the key factors that limit IDS adoption on high-speed networks and conducts a thorough analysis to show how IDSs perform in a variety of configurations, traffic levels, and flows. The difficulties of using open-source IDSs in high-speed networks have been thoroughly investigated, and proposals for assisting network administrators in resolving discovered concerns as well as recommendations for developing

new IDSs for high-speed networks are being explored.[20]
In recent years, the Internet-of-Vehicles (IoV) has emerged as an open and integrated network system for increasing transportation efficiency and reducing traffic congestion. Processing and frequent data interchange in Wireless Multimedia Sensor Networks (WMSN) demand energy-efficient and Quality of Service (QoS) assurances to support novel applications in the sensing layer of the Internet-of-Vehicles. Current routing methods do not account for energy usage while preserving QoS since WMSNs are heterogeneous and energy distribution is uneven. As a result,preserving QoS while improving energy distribution efficiency has become a difficult task. In this paper[21], In WMSN, the author presents a distributed adaptive cooperative routing that is energy-efficient, which not only provides QoS but also improves energy distribution efficiency.The adaptive strategy for assisting nodes in deciding whether or not to keep routing tables saves a significant amount of energy and allows for a more uniform distribution of energy.Simulation is used to test and compare the performance of the energy-efficient adaptive cooperative routing. The collected results show that energy usage is lowered while QoS is maintained when compared to older protocols.[21]
A profusion of picture editing software (such as Photoshop and others) has evolved with the rapid progress of digital technology, making the alteration of digital photos easier and more convenient.Sharpening with USM (Unsharp masking) is a popular technique for increasing image quality in digital image processing.The detection of USM sharpening in large-scale photos has recently been proposed as a method for identifying sharpening forgery. However, detecting sharpened images of small size remains a difficult task.In this paper [22], the author proposed an efficient USM sharpening detection technique for JPEG images with a resolution of 64 x 64 pixels. Converting the RGB image to a YCrCb image yielded the Y channel component. A block DCT transform was used to convert the Y channel image into the frequency domain. Following these steps, a difference matrix was used to generate the picture feature. Finally, for training and testing, the feature set was loaded into an SVM classifier. In small-size images, experimental results suggest that the proposed method outperforms the present method in sharpening detection[22].
Table 1 shows the advantages and disadvantages of certain investigations on Cloud, Wireless networking and block chain technology for high encrypted communications.
The notion of cloud computing is not new technology, it is continually evolving.Cloud concepts – ideas, software, and hardware – were established in the 1940s and 1950s by thinkers and inventors to answer some of the difficulties that had previously been theorised and explored. In the 1990s, cloud computing infrastructure was finally built.AWS was founded in the early 2000s, and the then-new EC2 service was released. Edge computing was facilitated by the emergence of "big data" technologies, among other factors.In the previous ten years, many more companies have entered the cloud scene to provide distinct cloud services, Microsoft Azure and Google Cloud Platform are two examples. It leaves a trail of devastation in its wake, developing industries like cloud-native programming, edge computing, and serverless infrastructure.
Property titles, music, insurance, tangible goods and commodities, and even your personal data may all be stored, distributed, and traded utilising blockchain technology. This technology will have a significant impact on the financial services business. We won't need to keep our transactions "pending" for three days if we use a decentralised database or a public registry like blockchain to authenticate the identities of all participants. Because the transaction and settlement would happen at the same time that the ledger was updated,

settlement would be immediate. There are numerous examples of this type of application. Identity management is perhaps the most common application of blockchain technology.

6. CONCLUSION

In this paper, Certain investigations on Cloud, Wireless Networking and Block Chain Technology for high encrypted communications are surveyed. In case of cloud, generic secure data storage model, client-side deduplication scheme, Bayesian Attack Graphs, cloud data deduplication scheme is been discussed along with its performance. And encryption techniques include GROSE approach, MCBE Scheme in the public key setting, dynamic Boolean SSE Scheme. In wireless networking, a WSN routing protocol based on clusters, a channel reservation and retrial policy for a dynamic spectrum access system, Mixed Integer Programming (MIP),In WMSN approaches, energy-efficient distributed adaptive cooperative routing is discussed. Bloch chain technologies like DV – PoA (designated – verifier proof of assets) and other networks like Vehicular and hoc networks – (HMAC), FASUS mechanism, PV/WEC Particle Swarm Optimization algorithm, SimpleStab, Online supervised method, UIPA, DNN algorithm, Snort and Suricata and finallythe performance of an efficient USM sharpening detection technique for JPEG images is investigated. The proposed algorithms and approaches provide considerably good performance, high security and high efficiency.

FUTURE SCOPE

Better Cloud Services, Security, Modular Software Development, Market Growth, and Virtualization are the future of cloud computing.The aforementioned projections show that cloud computing has a huge potential for expansion.Theutilisation of this technology is becoming increasingly important for businesses.They must, in reality, restructure and invest in coding standards that will allow for a smooth transition to the cloud.Cloud computing is also closely linked to concepts such as the internet of things.It becomes easier for IoT to ensure performance, security, and functionality when data is stored in the cloud. The network's speed, which regulates the rate at which data is acquired and processed, would be the only constraint.Everything else about cloud computing will fall into place if the network is fast.

MIMO, cognitive radio, multi-carrier modulation, and network coding are some of the key wireless communications technological trends that are expected to affect the next generation commercial wireless standards and, as a result, future military solutions.

The majority of blockchain technology's potential applications are in the field of cybersecurity. The data is protected and verifiable, despite the fact that the Blockchain ledger is open and dispersed.To eliminate risks such as illegal data manipulation, encryption is performed via cryptography.

7. REFERENCES

[1] S. K. Khare, “Fast-track message authentication protocol for DSRC using HMAC and group keys,” Applied Acoustics, vol. 165, p. 107331, Aug. 2020, doi: 10.1016/j.apacoust.2020.107331.

[2] W. Yin, P. Hu, W. Wang, J. Wen, and H. Zhou, “FASUS: A fast association mechanism for 802.11ah networks,” Computer Networks, vol. 175, p. 107287, July. 2020, doi: 10.1016/j.comnet.2020.107287.

[3] S. M., S. S., and A. Thomas, “Generic cost optimized and secured sensitive attribute

storage model for template based text document on cloud," Computer Communications, vol. 150, pp. 569–580, Jan. 2020, doi: 10.1016/j.comcom.2019.11.029.

[4] S.Maiti and S. Misra, "GROSE: Optimal group size estimation for broadcast proxy re-encryption," Computer Communications, vol. 157, pp. 369–380, May 2020, doi: 10.1016/j.comcom.2020.03.052.

[5] S.Malathi and K. Elango, "Implementation of dead beat controller using Particle Swarm Optimization for software defined network," Computer Communications, vol. 155, pp. 235–243, April. 2020, doi: 10.1016/j.comcom.2020.02.064.

[6] R.Yarinezhad and S. N. Hashemi, "Increasing the lifetime of sensor networks by a data dissemination model based on a new approximation algorithm," Ad Hoc Networks, vol. 100, p. 102084, April. 2020, doi: 10.1016/j.adhoc.2020.102084.

[7] G. Tian, H. Ma, Y. Xie, and Z. Liu, "Randomized deduplication with ownership management and data sharing in cloud storage," Journal of Information Security and Applications, vol. 51, p. 102432, April. 2020, doi: 10.1016/j.jisa.2019.102432.

[8] M. Cao, L. Zheng, W. Jia, and X. Liu, "Real-time video stabilization via camera path correction and its applications to augmented reality on edge devices," Computer Communications, vol. 158, pp. 104–115, May 2020, doi: 10.1016/j.comcom.2020.05.007.

[9] K. Acharya, "Secure and efficient public key multi-channel broadcast encryption schemes," Journal of Information Security and Applications, vol. 51, p. 102436, April. 2020, doi: 10.1016/j.jisa.2019.102436.

[10] Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects," Journal of Network and Computer Applications, vol. 163, p. 102635, Aug. 2020, doi: 10.1016/j.jnca.2020.102635.

[11] F.Pernici, M. Bruni, and A. Del Bimbo, "Self-supervised on-line cumulative learning from video streams," Computer Vision and Image Understanding, vol. 197–198, p. 102983, Aug. 2020, doi: 10.1016/j.cviu.2020.102983.

[12] N. A. Karim, Z. Shukur, and A. M. AL-banna, "UIPA: User authentication method based on user interface preferences for account recovery process," Journal of Information Security and Applications, vol. 52, p. 102466, June. 2020, doi: 10.1016/j.jisa.2020.102466.

[13] B.Asvija, R. Eswari, and M. B. Bijoy, "Bayesian attack graphs for platform virtualized infrastructures in clouds," Journal of Information Security and Applications, vol. 51, p. 102455, April. 2020, doi: 10.1016/j.jisa.2020.102455.

[14] Shruti and R. Kulshrestha, "Channel allocation and ultra-reliable communication in CRNs with heterogeneous traffic and retrials: A dependability theory-based analysis," Computer Communications, vol. 158, pp. 51–63, May 2020, doi: 10.1016/j.comcom.2020.04.055.

[15] P. Wanda and H. J. Jie, "DeepProfile: Finding fake profile in online social network using dynamic CNN," Journal of Information Security and Applications, vol. 52, p. 102465, June. 2020, doi: 10.1016/j.jisa.2020.102465.

[16] H. Wang, D. He, and Y. Ji, "Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography," Future Generation Computer Systems, vol. 107, pp. 854–862, June. 2020, doi: 10.1016/j.future.2017.06.028.

[17] X. Zheng, Y. Zhou, Y. Ye, and F. Li, "A cloud data deduplication scheme based on

certificateless proxy re-encryption," Journal of Systems Architecture, vol. 102, p. 101666, Jan. 2020, doi: 10.1016/j.sysarc.2019.101666.

[18] L. Sun, C. Xu, and Y. Zhang, "A dynamic and non-interactive boolean searchable symmetric encryption in multi-client setting," Journal of Information Security and Applications, vol. 40, pp. 145–155, June. 2018, doi: 10.1016/j.jisa.2018.03.002.

[19] N.Tekin and V. C. Gungor, "Analysis of compressive sensing and energy harvesting for wireless multimedia sensor networks," Ad Hoc Networks, vol. 103, p. 102164, June. 2020, doi: 10.1016/j.adhoc.2020.102164.

[20] Q. Hu, S.-Y. Yu, and M. R. Asghar, "Analysing performance issues of open-source intrusion detection systems in high-speed networks," Journal of Information Security and Applications, vol. 51, p. 102426, April. 2020, doi: 10.1016/j.jisa.2019.102426.

[21] D. Wang, J. Liu, and D. Yao, "An energy-efficient distributed adaptive cooperative routing based on reinforcement learning in wireless multimedia sensor networks," Computer Networks, vol. 178, p. 107313, Sep. 2020, doi: 10.1016/j.comnet.2020.107313.

[22] D. Wang and T. Gao, "An efficient USM sharpening detection method for small-size JPEG image," Journal of Information Security and Applications, vol. 51, p. 102451, April. 2020, doi: 10.1016/j.jisa.2020.102451.

[23] Y. Wadia, R. Gaonkar and J. Namjoshi, "Portable Autoscaler for Managing Multi-cloud Elasticity,"2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 2013, pp. 48-51, doi: 10.1109/CUBE.2013.19.

[24] C. Baun, M. Kunze and V. Mauch, "The KOALA Cloud Manager: Cloud Service Management the Easy Way,"2011 IEEE 4th International Conference on Cloud Computing, 2011, pp. 744-745, doi: 10.1109/CLOUD.2011.64.

[25] Abuhussein, H. Bedi and S. Shiva, "Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing,"2013 IEEE Sixth International Conference on Cloud Computing, 2013, pp. 958-959, doi: 10.1109/CLOUD.2013.132.

[26] M. Udin Harun Al Rasyid, F. A. Saputra, Z. S. Hadi and A. Fahmi, "Beacon-enabled IEEE 802.15.4 wireless sensor network performance,"2013 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), 2013, pp. 46-49, doi: 10.1109/COMNETSAT.2013.6870858.

[27] R. Miura et al., "Disaster-resilient wireless mesh network - Experimental test-bed and demonstration,"2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), 2013, pp. 1-4.

[28] M. V. Rameesh, P. Rajan and P. Divya, "Augmenting QoS in Outdoor Wireless Sensor Networks through Frequency Optimization,"2015 7th International Conference on Computational Intelligence, Communication Systems and Networks, 2015, pp. 39-44, doi: 10.1109/CICSyN.2015.18.

[29] N. Savitri, A. W. S. B. Johan, F. Al Islama A and F. Utaminingrum, "Efficient Technique Image Encryption with Cipher Block Chaining and Gingerbreadman Map,"2019 International Conference on Sustainable Information Engineering and Technology (SIET), 2019, pp. 116-119, doi: 10.1109/SIET48054.2019.8986084.

[30] M. Vaidehi and B. J. Rabi, "Design and analysis of AES-CBC mode for high security applications,"Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014, 2014, pp. 499-502, doi: 10.1109/ICCTET.2014.6966347.

[31] K. Nguyen, L. Lanante, Y. Nagao, M. Kurosaki and H. Ochi, "Implementation of 2.6 Gbps super-high speed AES-CCM security protocol for IEEE 802.11i,"2013 13th

International Symposium on Communications and Information Technologies (ISCIT), 2013, pp. 669-673, doi: 10.1109/ISCIT.2013.6645945.

[32] Z. Hamici, "Towards Genetic Cryptography for Biomedical Wireless Sensor Networks Gateways," in IEEE Journal of Biomedical and Health Informatics, vol. 22, no. 6, pp. 1814-1823, Nov. 2018, doi: 10.1109/JBHI.2018.2860980.

[33] R. G.S. and M. Dakshayini, "Block-chain Implementation of Letter of Credit based Trading system in Supply Chain Domain,"2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020, pp. 1-5, doi: 10.23919/ICOMBI48604.2020.9203485.

[34] Shivendra, K. Chiranjeevi, M. K. Tripathi and D. D. Maktedar, "Block chain Technology in Agriculture Product Supply Chain,"2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 2021, pp. 1325-1329, doi: 10.1109/ICAIS50930.2021.9395886.

[35] Y. Zhou, J. Shi, J. Zhang and N. Chi, "Spectral Scrambling for High-security PAM-8 Underwater Visible Light Communication System,"2018 Asia Communications and Photonics Conference (ACP), 2018, pp. 1-3, doi: 10.1109/ACP.2018.8596126.