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

Cryptography Techniques and Internet of Things Applications – A Modern Survey

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

[1]Robotics and Automation, Sri Ramakrishna Engineering College, Coimbatore,641022, India.
[2]Electronics and Instrumentation Engg., 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]shangkavi.g@gmail.com

Abstract.Cryptography's single most essential application in the internet of things is securing communication routes. Here are a few examples of how current encryption can help make the Internet of Things a safer and more trustworthy place. In this paper, Certain Investigations on Cryptography Techniques and Internet of Things Applications are been proposed. In cryptographic techniques, Verifiable computing based on proofs and verifiable computing based on replication, FPGA, Multivariate Cubic MC problem, image cryptosystem, CB-PBS scheme, LB-2PAKA protocol, MECC and DLMNN, SKMA-SC technique, EC-ACS Scheme, IoT cryptographic system, ECC-PKI, ESEAP, GEDMs, hybrid security strategy HS^2, query system based on proxy re-encryption, IoT network security using post-quantum cryptography techniques and IoT Applications likea combination of the Whale Optimization Algorithm and the Moth Flame Optimization (MFO), Shodan, Packet sniffing applications and network mapping tools, LAM-CIoT, LoRa+, LoRa Gateway by using chirp spectrum modulation scheme, RECLB algorithm, twin Peaks, WoT Store, a centralised inconspicuousFor real-time monitoring of a large population, an IoT-based device-type invariant fall detection and rescue system, In the standard model, decentralised attribute-based encryption is used, as well as an authentication system, CWD-WPT charging systems on a VANET network in a cloud and fog computing environment, CAPODAZ, SCF-CLSPE scheme, IoT cryptographic system, MQTT, Multi-Dimensional Access Control (MD-AC) scheme, IoT network security using post-quantum cryptography techniques, lightweight AKA scheme and ENPKESS method.

Keywords:Field Programmable Gate Arrays, Multivariate Cubic, Modified Elliptic curve cryptography, Deep Learning Modified Neural Network, Suppressed K-Anonymity.

1. INTRODUCTION

Cryptography is one of the technologies that must be used to create a secure VPN.Different implementations of the same basic algorithms can provide both encryption and authentication, ensuring that the two security peers on the VPN are who they claim to be. Data confidentiality can be ensured using one of two types of encryption algorithms: symmetric cryptography or asymmetric cryptography. In symmetric, or regular,

cryptography, the sender and receiver must exchange the key, which is confidential information needed to encrypt and decrypt data. The procedure by which two peers agree on a key over an unsecured manner can be troublesome because peers have no way of interacting privately until the key is agreed upon.By encrypting a communication with two keys, asymmetric cryptography, also known as public key cryptography, solves the problem of key exchange. Only another key can be used to decrypt encrypted data. Messages can be safely received by pressing a single key as a Public Key (for example, at the bottom of an email message) and keeping a second, Private Key, private. Anyone wishing to establish a secure connection can simply encrypt the recipient's public key, with only the intended recipient being able to decrypt the encrypted text and receive the initial message by providing an anonymous private key.

The Internet of Things (IoT) is the connectivity of physical items with electronics built in their structures, allowing them to communicate and detect interactions with one another and with the outside world.IoT-based technologies will provide higher levels of service and improve people's daily lives in the next years.Medicine, energy, genetics, agriculture, smart cities, and smart homes are just a few examples of how the Internet of Things has become entrenched.

More than 9 billion 'objects' (physical objects) will be connected to the Internet starting immediately. This number is anticipated to reach 20 million in the near future.

There are four main features used in IoT:
1. Low-power systems -Low battery consumption and great performance are two conflicting objectives that have influenced the evolution of electrical systems.
2. Using a computer with clouds -IoT devices generate a large amount of data, which must be stored on a reliable storage server. Cloud computing is useful in this situation.The data is processed and read, which gives us greater room to look for things like electrical problems or errors in the system.
3. Big data availability -We all know that the Internet of Things is heavily reliant on sensors, especially in real time.As these electronic gadgets become more widely used in many areas, they will generate a massive amount of big data.
4. Network connection -An Internet connection is required to communicate, and each visible object must be represented by an IP address. According to the IP name, however, there are only a few addresses available.This naming mechanism will no longer work when the number of devices grows. As a result, scientists are seeking for a new naming system to represent each visual object.

A Brief History Of Cryptography

Cryptology is a relatively new field of study.Although it has been used to hide secret messages for thousands of years, cryptology as a science (and possibly an art) only emerged approximately a century ago.

An inscription in the vast tomb of the honourableKhnumhotep II, Egypt, dated to around 1900 BC, is the first known proof of the use of cryptography (somehow).Instead of using more typical hieroglyphic symbols, the author used some unique ones here and there.The goal was not to hide the message, but to change its appearance to make it appear more respectable. Despite the fact that this text was not written on a secret typewriter, it did, in

fact, provide a translation of the original text, and it is the first to do so. In early significant communities, evidence of a specific application of cryptography has been found.

Julius Caesar was known for utilising some type of encryption to send secret communications to his military leaders who had been sent to fight as early as 100 BC.The Caesar cypher is likely the most well-documented substitution in the scholarly writings depicted in Fig. 1. (A cypher is a type of algorithm that is used to encrypt or decrypt data.)Each plain text (clear text message to encrypt) character in a replacement cypher is replaced by another character to generate a cypher text (cypher encrypted text).Caesar utilised a three-cipher swap as an exception.Each character has been replaced in three places, so 'A' has been replaced by 'D,' 'B' has been replaced by 'E,' and so on. The letters were folded in half.

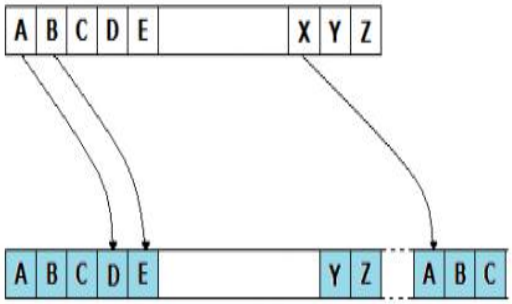

Fig. 1 Caesar cipher algorithm

It's clear that such cyphers rely on the system's secrecy rather than the encryption key.These encrypted messages can be readily decoded once the system is known.In reality, the frequency of letters in a language can be used to break substitution cyphers.

Vigenere created a cypher in the 16th century that is said to be the first to employ an encryption key like the one illustrated in Fig. 2. The encryption key was repeated numerous times across the entire message in one of his cyphers, and the cypher text was created by multiplying the message character by the key character modulo 26. (When one integer is divided by another, modulo, or mod, is a mathematical equation that calculates the remainder of the division.)Vigenere's cypher, like the Caesar cypher, is readily broken; nevertheless, The concept of encryption keys was introduced into the picture by Vigenere's cypher, however it was handled poorly. In contrast to Caesar cypher, the secret of the communication is determined by the secrecy of the encryption key rather than the system's secrecy.

Fig.2 Vigenere's cipher

Hebern invented the Hebern rotor machine, an electro-mechanical contraption, when everything became electrified at the turn of the century. A single rotor controls the secret key, which is hidden inside a rotating disc. Each keystroke on the keyboard produced cypher text, which was then encoded as a replacement table. The disc was also rotated one notch, necessitating the use of a new table for the following plain text character. This was once again broken using letter frequencies. Near the end of World War I, German engineer Arthur Scherbius created the Engima machine, which was heavily employed by German forces during WWII. Three, four, or even more rotors were employed in the Enigma machine. As you input on the keyboard, the rotors rotate at different speeds and emit the corresponding letters of encrypted text. The initial configuration of the rotors was crucial in this circumstance. Prior to WWII, most cryptography research centred on military applications, with the purpose of concealing secret military information. After WWII, however, cryptography garnered business interest as corporations tried to secure their data from competitors.

In the early 1970s, IBM formed a "crypto group" directed by Horst-Feistel after realising that their clients required encryption. Lucifer was created as a cypher. In 1973, the National Bureau of Standards (now known as NIST) in the United States issued a request for proposals for a block cypher that would become a national standard. They had clearly realised that they were purchasing a large number of commercial items that lacked adequate crypto support. Lucifer was eventually accepted, and the Data Encryption Standard (DES) was born.An intensive search attack broke DES in 1997 and the years that followed.The short size of the encryption key was the main problem with DES.It became easier to brute force all possible key combinations in order to get a plain text message as processor power increased.

In 1997, NIST released a fresh request for proposal for a new block cypher. There were 50 answers. Rijndael was accepted in 2000, and it was called AES, or Advanced Encryption Standard.

Milestones In Iot Evolution

ARPANET was the world's first connected network and the forerunner of today's Internet. ARPANET is where the Internet of Things got its beginnings.

David Nichols, a graduate student at Carnegie Mellon University's computer science department, In 1982, I was curious if the department's coke vending machine had cold soda bottles. He was tired of going to the vending machine only to find that no cold bottle was available; the vending machine was a considerable distance from his classes. As a result, he needed to know ahead of time.

Two fellow students, Mike Kazar and Ivor Durham, as well as John Zsarnay, a research engineer at the university, supported him in this endeavour. They could use the code they created to check if the vending machine had any coke and, if it did, whether it was cold or not. The state of the coke vending machine could be monitored by anyone on the university's ARPANET.

In 1989, Tim Berners-Lee proposed the World Wide Web Framework, which paved the way

for the Internet. In 1990, John Romkey created a toaster that could be turned on and off via the Internet. There was no Wi-Fi back then, so it was a toaster linked to the computer!! This toaster is regarded as the first IoT gadget, or the first "thing" that started the Internet of Things.

Caffeine - cold or hot - appears to have anything to do with researchers and scientists. In 1993, Quentin Stafford-Fraser and Paul Jardetzky created the Trojan Room Coffee Pot in a computer lab at the University of Cambridge. The inner image of the pot was uploaded three times per minute to the construction server. When browsers began to display images, these images were no longer viewable online. The term "Internet of Things" was coined by Kevin Ashton, the current CEO of Auto-ID Labs, in 1999.In terms of IoT architecture, this was a breakthrough moment. It was the title of a presentation he delivered at Procter & Gamble about tying RFID to the Internet in P&G's supply chain (where he was working at the time).

By 2003-2004, well-known publications such as The Guardian and Scientific American started adopting the term "internet of things."The US Department of Defense and Walmart both introduced RFID in their stores at the same time.The United Nations International Telecommunications Union recognised the importance of IoT in a 2005 report.The Internet of Things was predicted to contribute in the establishment of an entirely new dynamic network of networks.

In March 2008, Zurich hosted the first Internet of Things conference. To improve information sharing, it brought together academic and industry researchers and practitioners. In the same year, the US National Intelligence Council listed the internet of things as one of six disruptive civic technologies. The internet of things was completely born in 2008 and 2009, according to Cisco Internet Business Solutions Group (CIBSG), when the number of things linked to the internet surpassed the number of persons connected to it. The ratio of commodities to people increased from 0.8 in 2003 to 1.84 in 2010, according to the CIBSG.

Cisco also created a number of educational tools as well as marketing activities to entice clients interested in IoT adoption.
IBM and Ericsson quickly followed suit. In 2011, the Internet of Things was included in Gartner's Hype Cycle for Emerging Technologies. IDC predicted that the IoT business would increase at a CAGR of 7.9% by 2020, reaching USD 8.9 trillion, in a report issued in 2013.

Outsourcing a calculation has been commonplace since the introduction of cloud computing. To confirm that the findings are correct, two methods are used: (1) proof-based verifiable computing and (2) replication-based verifiable computing. The first approach, Proof-based Verifiable Computing, employs cryptographic techniques, while the second, Replication-based Verifiable Computing, use game-theoretic methods. Both methods have ideal options for checking or verifying the outcomes[1].

They look at the problem of verified cloud computing in this research. To ensure fairness, the bulk of existing systems rely on a trusted third-party. Blockchain technologies and smart contracts have inspired me. In this paper, methods for several verifiable computing techniques employing smart contracts are provided. The overhead of developing a smart-contract based solution for fair proof-based verifiable computation is relatively negligible when both the client and the cloud are honest.

Two distinct strategies are described, depending on the number of clouds used, to establish fairness in replication-based verifiable computing. Our protocols were developed using the Blockchain cryptography model, and their security was shown using universally composable theory. They also show the financial and transactional costs of proposed contracts by building them in Solidity and running them on the EthereumBlockchain[1].

Despite the immensity of IoT applications, a number of challenges must be addressed, including security, privacy, load balancing, storage, device heterogeneity, and energy management. Furthermore, the network's energy utilisation is critical and must be optimised. Residual energy, temperature, Cluster Head (CH) load, number of living nodes, and cost function all influence the energy consumption of sensor nodes.A hybrid Whale Optimization Algorithm-Moth Flame Optimization(MFO) is employed in this work to find the optimal CH. The results reveal that the proposed strategy outperforms earlier approaches [2].

The proper energy consumption of sensor nodes is critical for IoT networks' long-term viability. The proposed model's performance is compared to that of existing algorithms.The results reveal that the proposed model surpasses the others in all areas, including temperature, load, delay, energy, total number of alive nodes, and cost function. Future research could include more variables including network density, connection durability, and Quality of Service, as well as multi-objective optimization [2].

The goal of this research is to determine an attack surface for networks utilising Internet of Things (IoT) devices. The Internet of Things (IoT) is a network of devices that transmit and receive data without the need for human contact. Within the existing Internet infrastructure, each device can function independently. As devices become more common, problems will become more commonplace, and devices will continue to improve to counter newer threats and methods. All penetration points, also known as attack vectors, are summed together in a network's attack surface. These attack vectors can be used by an attacker to breach the threat environment and modify or extract data.They build a threat model for this study that allows them to methodically examine security solutions from the start of the design phase to mitigate potential hazards. They use IoT architecture and divide it down into multiple zones to detect any vulnerabilities or weaknesses inside a system that allow unauthorised privileges, as well as any assaults that can target that region.They also investigate the available IoT devices across many domains in order to develop a 1:1 and 1:n mapping between devices, vulnerabilities, and potential security problems based on subjective assessment[3].

Shodan, for example, scans the Internet for devices with open ports and keeps a database of them. Packet sniffing software and network mapping tools can be used to scan IoT networks for security problems such as plaintext passwords, open ports, and other vulnerabilities. Some device control interfaces are web-based and accessible to anybody. As part of minimising the attack surface, use obscurity and limit the availability of assets to allowed individuals. Our network model visualises the IoT network's danger environment by displaying trust zones and attack sites.The proposed methodology allows network security professionals to assess the risks associated with deploying new IoT devices while also providing potential solutions. The Internet of Things is constantly evolving, and new risks emerge on a regular basis[3].

In a cloud-based IoT ecosystem, data acquired via IoT sensors is saved on a cloud platform. This type of system is extremely scalable and enables for real-time event processing, which is crucial in a variety of situations (i.e., IoT sensors basedsurveillance andmonitoring). The data gathered and sent by IoT sensors must not be leaked during communication since some cloud-based IoT applications are mission-critical. They developed LAM-CIoT, a revolutionary lightweight authentication technique for cloud-based IoT systems, to achieve this goal. LAM-CIoT allows an authenticated user to remotely view data from IoT sensors. LAM-CIoT makes use of efficient "one-way cryptographic hash algorithms" and "bitwise XOR operations." A fuzzy extractor mechanism is also utilised at the user's end for local biometric verification. Finally, using the NS2 network simulator for the evaluation of network performance parameters, the impact of LAM-CIoT on the network performance of LAM-CIoT and other schemes is analysed [4].

Some Internet of Things (IoT) applications, such as healthcare, government, and military, require public key cryptography (PKC) services such as authentication, encryption, signatures, and key agreements. The most efficient approach for providing these services has been identified as elliptic curve cryptography (ECC). The simplest basic and most expensive operation in an ECC-based system is scalar multiplication (kP). To ensure that ECC meets the application requirements, it must be correctly implemented in IoT applications. This study presents an FPGA-based acceleration engine for primary ECC operations using binary Edward curves, which is suitable for use in limited devices (such as those in the IoT ecosystem). As main findings, the proposed system is light and general, needing less than 1400 slices of Virtex-5 FPGA while providing a security level similar to 128 bits. The described architecture, according to a literature assessment of comparable research, uses the least amount of FPGA hardware [5].

It was shown how to build and implement a hardware kP module for BEC curves.This design supports variable field lengths, scalars, and base points, polynomials, curve constants, exhibiting its versatility. The architecture shown here runs in real time, providing some protection against side-channel assaults [5].

The proposed architecture was analysed in terms of hardware use and compared to relevant studies in the literature. Based on this comparison, the suggested architecture is appealing for space-constrained applications, such as those found in the IoTecosystem[5]. The kP architecture described here supports generality to a significant extent, with hardware costs of less than 1500 SLC and run-times of less than 10 ms for adequate security levels. The results are the product of the paper's careful design and implementation procedure[5].

Table 1
The implementation results for the proposed architecture using two binary Edwards curves for over the field F_2251 on the Artix 7 and Virtex 7 FPGAs.

Conf.	FPGA	Curve	FF	LUT	SLC	LAT	WNS (ns)	t (ms)	POW (mW)	ENE (mJ)
C1	XC7A	BE251	2149	4280	1418	832,818	1.501	8.33	84	0.70
	XC7VH	BE251	2149	4109	1327	832,818	2.227	8.33	700	5.83

C2	XC7A	BE251-b	2114	4017	1329	824,284	1.479	8.24	83	0.68
	XC7VH	BE251-b	2114	4013	1288	824,284	2.395	8.24	700	5.77

The design of the suggested structures is outlined in three ways in this paper:

1. We used two elliptic curves that are very easy to change. According to Table 1, resynthesizing the design for the BE251-b curve can provide certain hardware benefits. By simply providing the right curve constant as input, the C1 configuration may function with both BE251 and BE251-b on the fly. Any binary Edwards curve can be used in the suggested design, illustrating the elliptic curve's adaptability.

2. A comparison to the State-of-the-Art was provided for various field lengths. These findings, as given in Table 2, illustrate that the proposed architecture can adapt to changing security levels while balancing space and performance trade-offs.

3. The suggested architecture was tested on four FPGAs and two design toolchains to prove that it achieves similar implementation outcomes across platforms. This is due to the fact that the designs created as part of this project are very portable.

Low area was the key optimization target during the design phase; nevertheless, this does not mean that the realisation delay was completely ignored. This may be seen in the choice of a combinatorial addition layer, which can be used due to the rigorous design technique used. Although the proposed design is not well suited for high-performance applications, it may be appealing in situations when space is constrained. Furthermore, the suggested design's reconfigurability provides a number of advantages for security applications:One piece of code can be optimised to optimise a variety of architectures, each of which can be customised to match the needs of a particular application. The proposed solution can be described as lightweight [5] based on the implementation results and the design process followed.

The LoRaWAN (Low Power Wide Area Network) protocol is a commonly used LPWAN (Low Power Wide Area Network) protocol for the Internet of Things (IoT).The MAC layer protocol for LoRa is called LoRaWAN.Certain measurable Quality of Service (QoS) improvements, such as the rate of rejected packets and the Packet Error Rate (PER), are still needed (PER). In their study, they proposed a LoRa+ as a new mechanism to remedy the shortcomings of LoRaWAN. Currently, at the end of each uplink operation, a conventional LoRaWAN-based end device opens two time slots (RX1 and RX2) to receive the channel characteristics from the gateway: the spreading factor and the operational frequency. These factors must be taken into account when the next uplink occurs, which could be a few hours later (highly application dependent). The channel conditions may change throughout this time, reducing performance.

They modified the LoRaWAN MAC Layer for both Class A and Class B to solve this problem.The time window for receiving channel parameters has been altered such that they are transmitted shortly before the transmission slot, rather than waiting until the uplink procedure is complete. Using Matlab simulations, they show that our adjustment reduces the rejected packet rate and PER by up to 20% when compared to LoRaWAN for small and medium-sized towns with less than 500 EDs.

As a result, the network's necessary number of gateways is lowered, cutting network infrastructure costs [6].

They introduce a novel technique dubbed LoRa+ in this work to increase the LoRaWANQoS.After describing the LoRaWANtechnology and its classes, they highlighted the problems of transmitting over a channel before collecting the parameters from the GW. This flaw raises the rate of rejected packets in the LoRaWAN network and reduces the GW's radio reach. After the architecture of the LoRaWAN standard is given, the proposed LoRa+ mechanism is demonstrated and discussed. After that, a system model was created to compare LoRaWAN and LoRa+ in a variety of scenarios (urban and rural). In comparison to LoRaWAN, the results suggest that the new LoRa+ mechanism is more efficient. LoRa+ enhances connection between the ED and the GW while reducing collisions and interference. In a region with high ED density, it also allows LoRa network operators to cut the number of GWs by up to 80%, resulting in significant cost savings. Those emperical results are highly encouraging, thus an actual implementation in the near future is on the cards [6].

With the advent of internet technology, society has begun to seek for e-mechanisms such as e-voting, e-commerce, and e-learning, among others, in which electronic data is exchanged between entities via a public network. E-mechanisms, on the other hand, necessitate that the sent electronic data be of high integrity, authenticity, and non-repudiability. The digital signature is a method of obtaining these qualities while sending data over a public network. Existing number theoretic assumption-based digital signature systems are vulnerable to quantum attacks as a result of the development of a quantum computer. MPKC-based structures are computationally rapid and require only a modest amount of computer power, making them one of the most promising post-quantum cryptography alternatives.In the literature, there are only a few multivariate digital signature algorithms based on the Multivariate Quadratic (MQ) problem.However, developing viable digital signature systems based on multivariate polynomials of greater degree (> 2) is still a work in progress.Multivariate polynomials with degrees more than 2 are expected to be equally as difficult as quadratic polynomials. Under the same security assumptions, the signature size of their system is smaller than all other MPKC-based signature schemes [7].

The MQ problem is a subset of the MC problem, which has less solutions than the MQ prob-8 N. As a result, the MC problem is expected to be similarly complex in terms of security as the MQ problem. There is no multivariate digital signature scheme based on the MC problem that we are aware of. In this paper, we address this problem by developing OHV, a digital signature system that achieves post-quantum security under the MC problem. Furthermore, for the same level of security, the signature scheme provides the appropriate signature size [7].

This study proposes a cloud-based digital image locker system with secure user identification and a unique image cryptosystem for safeguarding the privacy of user photos. When compared to words, images require greater storage space. As a result, storing photographs locally in a digital locker is not viable for everyone. Using high-speed Internet, it is possible to leverage the cloud for efficient image storage.Cloud technology, on the other hand, is viewed as "honest but weird" by many academics. The cloud service not only follows the protocol to the letter, but it also traces and analyses the data in order toretrieve the user's vital data. To overcome these barriers, a user's identity and data must be kept private. The

proposed authentication process uses a Paillier-based difference function and is based on the Homomorphiccryptosystem.

The unique feature of homomorphic functions is that they can be used to compute encrypted data without having to decipher the cypher text. As a result, the authentication procedure takes place in a secure environment. A novel picture cryptosystem is created using the Fridrich model. In this cryptosystem, confusion occurs at the bit level, while diffusion occurs at the pixel level. Each round of consternation results in the modification of keys in order to increase security. The suggested system's effectiveness is demonstrated through simulation and cryptanalysis [8].

The proposed authentication protocol uses the Secure Hash Algorithm (SHA-256) and a Paillier-based difference function to ensure that the authentication process takes place in an encrypted environment. Brute force, dictionary, advanced dictionary, lookup table, and rainbow table assaults are all resistant to the proposed authentication scheme. To secure image privacy, a novel image cryptosystem is proposed and implemented. The proposed picture cryptosystem uses chaotic maps as input and a seed value generated from a simple image.

Table 2
The implementation results for the proposed architecture and comparison with related works that use BECs. The costs reported are associated with performing *kP*in each case.

Ref.	Year	Platform	Constants	*m*	Digit	FF	LUT	SLC	GE	Cycles	*t*(ms)	
	MHz											
Offering less than 112 bits of security.												
[7]	2010	130nm	$d_1=d_2$	163	1	-	-	-	11720'	219,148	0.54	400
[10]	2012	XC5VLX	$d_1=d_2$	163	21	2771	8158	3181	-	7915	0.03	269
			$d_1/=d_2$	163	21	3097	8158	3181	-	10,041	0.04	269
[12]	2015	XC5VLX	$d_1=d_2$	163	-	-	10,086	-	-	-	0.5	318
[3]	2015	65nm	$d_1=d_2$	163	1	-	-	-	11,219	177,707	-	-
[13]	2016	XC6SLX	-	163	-	-	-	-	14,200	23,023	23.02	1
Ours	2019	XC6SLX	$d_1=d_2$	163	1	1414	2727	840	8083	351,591	3.39	104
		XC5VLX	$d_1=d_2$	163	1	1428	3087	1123	8083	351,591	2.69	131
Offering 112 bits of security.												
[12]	2015	XC5VLX	$d_1=d_2$	233	-	-	15,804	-	-	-	1	308
[3]	2015	65nm	$d_1=d_2$	233	1	-	-	-	15,177	351,856	-	-
[14]	2016	XC5VLX	$d_1=d_2$	233	-	-	-	-	-	-	0.003	132
[31]	2017	XC5VLX	$d_1=d_2$	233	78	-	-	1343'	-	126983	0.343	370
		180nm	$d_1=d_2$	233	78	-	-	-	29524'	126983	0.118	1071
Ours	2019	XC6SLX	$d_1=d_2$	233	1	1995	3878	1245	12149	718,805	6.72	107
		XC5VLX	$d_1=d_2$	233	1	2010	4340	1397	12149	718,805	4.56	158
Offering more than 112 bits of security.												
[3]	2015	65nm	$d_1=d_2$	283	1	-	-	-	19,332	512555	-	-
[15]	2019	XC6SLX	$d_1=d_2$	251	16	2177	7251	2099	-	29094	2.15	13.56
Ours	2019	XC6SLX	$d_1=d_2$	251	1	2138	4122	1357	12,410	832,818	7.62	109
				251	1 115	2102	4069	1351	12240	824,284	7.17	
		XC5VLX	$d_1=d_2$	251	1	2153	4644	1396	12,410	832,818	5.32	157
				251	1 162	2117	4539	1369	12240	824,284	5.10	

In some cases, only the results with the smallest area were retrieved. The blank spaces "-" represent data not available in the respective work. The marker "' " represents that additional storage is required.

In some cases, only the results with the smallest area were retrieved. The blank spaces "-" represent data not available in the respective work. The marker "*" represents that additional storage is required.

In 2003, C. Gentry introduced the certificate-based encryption (CBE) paradigm to combine the benefits of PKC and identity-based PKC (ID-PKC). CBE also solves the escrow and secret key distribution concerns of ID-key PKC, as well as PKC's third-party inquiry problem. This article presents the first short and efficient provably secure certificate-based proxy blind signature (CB-PBS) method based on pairing over elliptic curves. The suggested CB-PBS system is proved to be secure under adaptively generated message and ID assaults in the random oracle scenario. Because of its short length, it is the most appealing to employ in low bandwidth communication systems to build e-cash, e-voting, and other applications [9].

In the ROM, the proposed strategy has been proven EUF-ACMA against three types of formidable attackers. In the literature, the bulk of CB-PS approaches use a certification by delegation technique, which is inadequate for today's applications.They provided a plan that was unrelated to this strategy, but our plan made full advantage of delegation. The proposed system is shown to be the most efficient and brief CB-PBS technique, with the added benefit of being free of key escrow, secret key distribution, and third-party inquiry problems. Due to the significant cost of pairing, creating a pairing-free short CB-PBS scheme [9] is an open problem.

The two-party authenticated key agreement (2PAKA) protocol is a cryptographic tool that allows two users to generate a shared and unique session key for each of their sessions over an unsecured network. The authenticated variation of a two-party key agreement system is popular because it can easily withstand user impersonation. Many 2PAKA techniques have been presented in the literature based on the discrete logarithm (DLP) and integer factorization issues' intractability assumptions (IFP). Recent investigations in post-quantum situations have revealed that 2PAKA protocols based on these assumptions are weak. The

proposed LB-2PAKA protocol is further tested in a random oracle model to determine its proved security and breaching time. They used the LatticeCrypto Library to estimate the LB-2PAKA protocol's execution time in order to assess its performance. They also looked into the LB-2PAKA protocol's communication cost requirements[10].

The LB-2PAKA protocol provides provable security in the random oracle concept. According to our proven security analysis, the probability of an adversary infringing on the semantic security of the session key is negligible, and the time necessary is more than the time required to address the RLWE issue. They also use the Lattice Crypto Library to look at the LB-2PAKA protocol's execution time. Their LB-2PAKA protocol, they believe, will be more suitable for many Internet-based applications in post-quantum contexts than existing 2PAKA protocols [10].

VCC stands for vehicle cloud computing and encompasses cloud, vehicular networking, and Internet of Things (IoT) technologies. vehicle-to-infrastructure,Vehicle-to-vehicle, and vehicle-to-device communication are all examples of VCC, in which vehicles have communication sensing capabilities. VCC makes use of vehicle resources, cloud infrastructure, and the Internet of Things. However, ensuring communication security and communicators' privacy are two important issues in VCC.They propose a VCC authentication framework based on elliptic curve cryptography (ECC) and equipped with a radio frequency identification (RFID) to achieve the goal of secure communication while keeping anonymity [11].

They demonstrated that the suggested approach assures secure communication utilising formal security analysis in the random oracle model and information security analysis. We also demonstrated the proposed protocol's security against replay attacks and man-in-the-middle assaults using the simulation tool "AVISPA." On desirable performance metrics, we evaluated the proposed framework's performance and compared it to analogous systems. According to our findings, the suggested system satisfies all desirable security properties while also facilitating effective communication[11].

In today's digital age, it's critical to consider how new long-range communications services have been enabled by the Internet of Things (IoT), especially as the number of linked devices expands in the future. Although numerous technologies are linked with low-power wide-area networking (LPWAN), long-range WAN is the most extensively utilised LPWAN technology because it provides higher connectivity for outdoor IoT applications while keeping network structures and management as simple as possible.This study [12] examined the system level outage of a single LoRa Gateway using the chirp spectrum modulation approach, as well as the coverage probability for multiple LoRa Gateway situations.

The key advantage of LoRa over other LPWAN is that it employs an adaptive CSS modulation method that extends the communication range if there is no interference on the channel, which is frequently exacerbated by the presence of LoRa gateways. In the experiment, the conditional and unconditional outage probabilities are plotted versus distance, and the results show that the conditional outage probability decreases while the unconditional outage probability increases.A closer examination of the behaviour of the obtained results reveals that the second outage probability has a bigger influence on both the outage and coverage probability. The study also discovered that adding other LoRa gateways

in the same geographical region reduces the LoRa Gateway's overall performance even further.[12]

Anti-forensics is a collection of strategies and procedures used by an attacker to thwart the digital investigation process in a computing environment. Anti-forensic attacks frequently target cloud computing infrastructures, disrupting the cloud forensic process and tampering with evidence, resulting in investigational damage. In this paper, the author developed approaches for secure data transfer and early detection of anti-forensic threats in the cloud using Modified Elliptic Curve Cryptography (MECC) and Deep Learning Modified Neural Networks (DLMNN). The proposed MECC has a security rating of 96 percent, compared to 90 percent for the present ECC and 87.5 percent for the existing RSA-based approach. On the receiver side, the author recommended the Modified Elliptic curve cryptography (MECC) technique, which encrypts data packets and transmits them to a receiver, where the packet IP address is determined by a Deep Learning Modified Neural Network (DLMNN) classifier. Based on the sender's IP address, DLMNN assesses if the received packet is attacked or not. [13]

When using cloud data services, maintaining security and privacy is a major issue that must be addressed. This paper[14] proposes a novel multi-factor authentication technique called Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography (SKMA-SC) to overcome the limitations of existing authentication techniques in which the client identity is verified by using a non-efficient single authentic authentication factor.

The client's sensitive information from third parties in the cloud environment is safely stored in the cloud server during the registration step of the SKMA-SC approach. During the authentication phase, clients' identities are verified using multifactor authentication methods such as passwords, one-time tokens, and conditional characteristics. The data access phase allows the customer to acquire requested data services utilising the Schmidt-Samoa data encryption/decryption procedure, which prevents unauthorised access from a third party in a short amount of time via an insecure communications cloud environment.Using computational complexity (CC) and privacy-preserving rate (PPR), the author assesses the performance of the SKMA-SC technique with various numbers of clients and cloud data, and the experimental results are quite promising.
[14]

The Internet of Things (IoT) encompasses a wide range of services, such as home management, in which a massive quantity of data is collected from a variety of smart devices and processed in scalable, high-performance, and fault-tolerant computer systems, such as cloud computing platforms.By replicating each application process over multiple virtual computers in a server cluster architecture, users can get dependable IoT services. Furthermore, a server cluster system with process replicas consumes more electric energy than a server cluster system without replicas, resulting in server cluster systems that are not only fault-tolerant but also energy-efficient. The authors of this paper[15] proposed a redundant energy consumption laxity based (RECLB) algorithm for redundantly and energy-efficiently completing each application operation on numerous virtual machines.The authors assessed the RECLB algorithm in both homogeneous and heterogeneous server clusters in terms of total electric energy consumption and average computation time for each process. [15]

In this study [16], the author suggests twin Peaks, an infrastructure for distributing public keys of named entities over the internet and internet of things (IoT) to address concerns such certificate revocation overhead and the impact of false certifications on the current public key infrastructure (PKI). TwinPeaks employs certificateless public key cryptography (CL-PKC), in which a key generation centre (KGC) is unaware of its members' private keys and hence the system cannot be hacked. TwinPeaks overcomes the PKI's flaws by distributing the public key of each identified entity online.

TwinPeaks features public key servers that form a hierarchical tree structure similar to that of the domain name system (DNS). For each parent-child connection in the DNS hierarchical tree, the parent node functions as a key generation centre (KGC), and the child nodes interact with the KGC to generate their own public/secret key pairs, as recommended by CL-PKC. Every named entity (such as a domain name) now has its own set of public and private keys. As a result, the public key of an entity will be distributed to users by its key server, just as the DNS response is delivered to the user by the DNS server. Twinpeaks' public key is based on both its IP address and domain name, therefore impersonation by a single organisation (such as a DNS or key server) is impossible. By extending the naming strategy, this study also shows how TwinPeaks can be applied to IoTcontexts.[16]

The Internet of Things (IoT) has generated a fragmented landscape around the world, with a vast variety of devices, technologies, and platforms, as well as interoperability difficulties on numerous system implementations. The Web of Things (WoT) architecture recently presented the W3C consortium with a breakthrough method to enabling interoperability across IoT systems and application domains. The creation of well-defined and comprehensive support tools for deploying W3C WoT applications is also required by the widespread acceptance of W3C WoT solutions by academic and industry communities [17].

This article proposes the WoT Store, a new platform for managing and simplifying the deployment of Things and applications on the W3C Web of Things (WoT). This allows for dynamic discovery of the resources available in the environment, i.e. the Things, as well as interaction via a dashboard, which includes displaying their properties, issuing commands, and monitoring the generated notifications. The WoT Store also makes it easy to find and use third-party WoT programmes that interact with the things that are available. The authors also used two evaluation studies to validate the proposed framework's operations: the first used a small-case testbed to demonstrate Thing discovery and the ability to run WoT applications that orchestrate the operations of multiple, heterogeneous Wireless Sensor Networks (WSNs), and the second used a mixed real/simulated large-scale crowdsensing simulation. [17]

As the world's elderly population expands, using technology to create precise and fast automatic fall detection systems has become a necessity. The bulk of fall detection systems are designed for specific devices, which limits the versatility of the system. This study proposes a centralised, unobtrusive IoT-based device-type invariant fall detection and rescue system for real-time monitoring of a large population. Any device, such as smartphones, Raspberry Pis, Arduinos, NodeMcus, and Custom Embedded Systems, can be used to monitor a large population in the proposed system. The devices are kept in the user's left or right pant pocket. The accelerometer data from the devices is continuously sent to a

multithreaded server, which runs a machine learning model that analyses the data to see if a fall has occurred. The server sends the classification results back to the devices. The server sends an SMS to the mediator alerting them of the user's location if a fall is detected. As a failsafe, the associated device sounds the alarm to alert nearby people and sends an SMS to emergency medical services and mediators, resulting in the user's life being saved. The proposed method had a 99.7% accuracy rate, a 96.3 percent sensitivity rate, and a 99.6% specificity rate. Finally, because no external connections are required, the proposed system may be used to successfully monitor a large population with a low false alarm rate without interfering with users' daily life [18].

The designed system is extremely fast, with a response time of about 190 milliseconds. This means that within 190 milliseconds of delivering motion data to the server, the server and client's device know if a fall has occurred or not [18].

Attribute-Based Encryption (ABE) has grown in popularity as a cryptographic method for fine-grained access control in a range of applications, including Cloud-assisted IoT data transmission. A decentralised ABE with untrusted attribute authority is proposed to replace the online Trusted Authority (TA). A data client (for example, an IoT device) presents his attributes to an untrusted authority in order to receive the private keys in a decentralised architecture. User privacy in the face of shady authorities is a major worry that must be addressed in the design (e.g., E-health Cloud application). In this work, they address the privacy issue in the distributed ABE, and they provide a novel anonymous and decentralised attribute-based encryption in the conventional model. It effectively protects the user's anonymity from government officials. They use cryptographic accumulators in their approach to anonymously validate the user's attributes. To safeguard the ABE access control from unauthorised users, the accumulator is then incorporated in the ciphertext. Furthermore, certain applications' access structures (encryption/decryption policy) contain sensitive data that should be hidden from all users except those with secret key qualities that match the access structures. They offer a decentralised policy obfuscation mechanism to safeguard the policy's privacy from the Public Cloud Server, ensuring that the hidden policy is protected (PCS). It's thrilling to work in a decentralised system where authority can't be trusted and may conspire with the PCS. They offload the expensive decryption computation to powerful Cloud servers in order to be usable for IoT devices with little resources. Then they formally assess the proposed scheme's security features and undertake experiments to demonstrate its efficacy. Finally, they briefly describe how the proposal's features satisfy the needs of various real-world applications [19].

To be usable for cloud-assisted IoT networks with resource-constrained devices, the decryption expense was outsourced via cloud servers. Under the proposed approach, the user's privacy is totally preserved.Both identity–anonymity and attribute–anonymity are secured against untrusted attribute authorities during the creation of private keys. In addition, a novel obfuscating distributed access structure ensures hidden policy, such as the privacy of an expressive access-structure against the PCS. As a result, the PCS, in conjunction with untrustworthy authority (at most N 2), is unable to decipher the policy contained in the ciphertext.Finally, they give their security proofs and efficiency analysis, as well as a brief overview of their scheme's applications in several exciting real-world circumstances. Specific application enhancements will be left for future work [19].

The integration of these technologies has become a promising field with a number of issues, including security, with the rise of Smart Cities and underlying adoptions of technologies such as the Internet of Things and Cloud Computing. One of the most prominent initiatives to address these challenges is authentication. Allowing direct device-to-device connections rather than only device-to-service communications has a number of benefits, including greater data transmission rates and more consistent connectivity even when central clouds fail. The resource-constrained nature of IoT devices, on the other hand, makes developing safe protocols that can be deployed in practise more difficult. This paper provides an authentication system extension that allows for secure control of devices from resourceful cloud servers as well as direct secure communication between them. The concept is aimed to enable efficient resource and energy usage through the use of ECC and low-cost operations. To demonstrate the protocol's correctness, a rigorous security analysis using BAN-logic is employed. A detailed study is provided to demonstrate the system's resistance to typical attacks. A performance investigation demonstrates the scheme's practical worth, revealing that it consumes no more than 29 mJ on each device in addition to the amount required by the original protocol.[20]

We also performed a theoretical deep analysis (based on the BAN-logic (Burrows et al., 1989) to show that the newly proposed approach is safe and may be used to light-weight embedded devices. These findings suggest that their innovative proposed strategy outperforms previous work in a variety of real-world application areas, particularly in smart cities and resilient environments. [20]

The Internet of Things (IoT) has advanced at a dizzying rate in recent years, becoming increasingly sophisticated. Because they allow various items to speak with each other, Communication Things Networks (CTNs) are a fundamental component of the Internet of Things (IoT) (between objects or objects with the internet). The introduction of novel services like charge while driving (CWD) based on wireless power transfer (WPT) technology is a pillar for the growth of CTNs in the context of electric vehicles. One of the networks that can support the CWD-WPT system's high mobility, low latency, and connection is cloud-based vehicular ad hoc networks (VANETs). The CWD-WPT charging system provides consumers with convenience and time savings if the system's privacy, integrity, and availability are guaranteed. This paper proposes an authentication methodology for a CWD-WPT cloud charging system that employs numerous cryptographic algorithms for key management and distribution, message privacy and integrity, mutual authentication of system elements, and EV anonymity [21].

This article addresses network security and access control in cloud-based vehicle networks, ensuring that the most important security criteria, such as authentication, data integrity, confidentiality, access control, non-repudiation, and availability, are addressed. The purpose of this research is to contribute to the optimization and security of vehicular networks that support electric cars (EVs), which have become popular in a number of countries as a result of the global goal of reducing air pollution. For CWD-WPT charging systems on a VANET network in a cloud and fog computing environment, the manuscript established a new authentication mechanism based on digital signatures, HMACs, and hashing chains. A brief review of some work on authentication in CWD-WPT charging systems [21] is also included.

In compared to other approaches, their solution is less expensive to implement and provides

superior security and safety analysis results, as well as eliminating worries about centralization caused by the use of a cloud environment that combines fog and cloud computing. The computational processing of processes in the devices is divided more evenly as a result of this combination, and communication latency is reduced. The protocol has met the security objectives, according to a formal verification performed using the AVISPA tool [21].

In terms of designing agile apps and providing complex solutions, the microservices architecture paradigm offers substantial benefits. However, suitable access control procedures and authorizations must be implemented in order to transmit information and communicate data between services in a verifiable and stateless manner. We examine how policy-driven authorizations interact with independent fine-grained microservices in a real-world machine-to-machine (M2M) scenario with a hybrid cloud-based architecture and Internet of Things (IoT) services in this study. They also propose a containerized authorisation and policy-driven architecture (CAPODAZ), which is built on the microservices paradigm and models the authentication flows that allow message exchanges between relevant entities. In the current development of a Cloud-IoT intelligent transportation service, the proposed architecture integrates a policy-based management structure. They compare the proposed architecture to other similar microservices and treat multiple user population distributions for in-depth quantitative evaluation. Numerical results based on experimental data show that there is a significant performance majority in terms of latency, throughput, and successful requests [22].

In this paper, they introduced a cloud-based containerized authorisation and policy-driven architecture (CAPODAZ). CAPODAZ, which is integrated into the iBuC intelligent transportation service prototype, encapsulates our previous work on the SeMMA architectural characteristics. They used a capability token-based system to make authorisations easier and put CAPODAZ to the test in a real-world IoT environment for intelligent transportation services. The suggested design was then compared to various microservice frameworks, with a focus on load-level latency, throughput, and successful requests. They employed the Docker built-in engine for intra-microservice messaging, which depends on the Linux operating system's processes synchronous communication. CAPODAZ was shown to be the best-suited framework for a group of 1,000 users, which is a suitable population size for the analysed real-life scenario. The best CAPODAZ performance was shown in the most realistic scenario (Poisson), in which the load was irregularly time-distributed and requests arrived at a fast rate. The suggested microservice architecture can be implemented in any cloud-based environment due to its containerized nature [22].

A new information service mode is provided by the smart healthcare system (SHS). It considerably enhances diagnostic efficiency by continuously monitoring patients' vital signs using a variety of wearable devices. In order to protect the confidentiality of sensitive data, security and privacy issues have attracted a lot of attention. Searchable encryption technology is suitable for addressing these problems because it allows for search across encrypted data while also protecting data privacy. To establish a compromise between security and efficiency, many searchable public-key encryption (SPE) algorithms have recently been created. Certificate management or key escrow, on the other hand, is a challenge for these SPE methods. This is the case because they are based on a public key infrastructure (PKI) or identity (ID) cryptosystem. Meanwhile, most SPE approaches are

susceptible to attacks like as keyword guessing (KGA). To overcome the aforementioned difficulties, this paper offers a SCF-CLSPE method, which is a secure certificateless SPE technique for SHS that does not rely on secure channels. They demonstrate that, in the traditional model, this SCF-CLSPE approach can withstand KGA and keyword attacks (CKA). The results of the performance analysis also demonstrate that the SCF-CLSPE scheme is more efficient [23].

With the rise of IoT and the increased use of smart terminal devices, the SHS system presents a brand-new information-based healthcare service platform. It has more advantages than traditional health-care approaches, such as allowing medical resources to be shared and minimising registration wait times. People benefit from SHS because it makes healthcare more accessible, but it also raises issues about data security and privacy. To overcome these difficulties, they create a SCF-CLSPE scheme for SHS that is secure against KGA attacks and can withstand CKA attacks under the usual model. Furthermore, they assess the suggested SCF-CLSPE scheme's performance. According to the performance analysis, the proposed system is nearly identical to Lu et alscheme, .'s and our proposed scheme is more efficient in the encryption phase than Rhee et al.'s scheme. Despite performing somewhat worse in the test phase than Lu et al.'s approach, the recommended technique can achieve IND-CKA security without the use of a random oracle [23].

Electronic Health Records (EHR) have lately emerged as a critical component of the E-health care system, allowing healthcare practitioners to exchange patient health records through a gateway of their choosing. In this scenario, a lack of confidentiality and integrity features leads to a slew of security issues with sensitive health data, all of which have a substantial impact on a patient's life. To secure EHR employing authorisedblockchain technology, they offer the Elliptical Curve Certificateless Aggregate Cryptography Signature technique (EC-ACS) for public verification and auditing on the Medical Cloud Server (MCS). They use Elliptic Curve Cryptography (ECC) to encrypt medical data and the Certificateless Aggregate Signature Scheme to establish digital signatures for sharing and storing data in cloud storage (CAS). This recommended technique assures security, privacy, and protects personal information from unauthorised access in the cloud health system. The blockchain solution also protects the integrity, traceability, and safe storage of medical records in the cloud [24].

In the healthcare industry, medical records contain personal information about patients that should not be shared with outsiders. As a result, the medical cloud was built to keep medical records safe, but it might be manipulated by third parties, such as impostor doctors, who would remove and alter the original data. As a result, they proposed an EC-ACS public verification and auditing method in the MCS in this work, using authorisedblockchain technology. To begin, the secure certificateless public verification approach encrypts and verifies the aggregate signature using ECC for key creation and data signature verification. Then they design a secure certificateless public auditing system to verify that the data integrity of data outsourced via CSP is reviewed by a blockchain transaction auditor. To simulate their suggested technique, they employ the MATLAB software. In this, they consider indications like calculating cost, verification, aggregation, and auditing delay. According to the performance comparison, their scheme is more efficient on the side of the TPA, which is more lightweight and suitable for cloud-based HER [24].

With each passing day, the Internet of Things (IoT) has the potential to transform our

civilization into a more digital one. This study provides a cryptography system based on IoT-optimized technology that has been designed and implemented. Because of the multiple advantages of IoT, it is more than vital to establish a privacy platform. This project intends to illustrate this by first building efficient and adaptable cryptographic and privacy primitives. Second, this is accomplished by presenting applied cryptography in a more participative and flexible manner. The suggested system, as well as the platform's integration, are scrutinised. This paper introduces a symmetric cryptography application based on the Advanced Encryption Standard (AES) in the Electronic Code Book (ECB), Cipher Block Chaining (CBC), and Counter (CTR) modes of operation for text, image, and electronic data encryption and decryption. The suggested system also supports two further security schemes: AES Galois/Counter Mode (GCM) and AES Galois Message Authentication Code (GMAC). The GCM recommended incorporating it into an authentication mechanism that would ensure both authenticity and confidentiality. GMAC, on the other hand, is a message authentication code that can be used. Both procedures are optimised in terms of implementation resources, as the AES core is the most expensive component. Furthermore, based on the embedded hardware modules, user registration and validation is proposed and implemented at no additional cost and with no performance impact.
Also built and shown is a two-factor authentication system based on One-Time Passwords (OTPs) that can be produced using a random manner. Following that, there's a mention of security levels in terms of communication across the architecture's IoT layers. Because IoT hardware platforms have a low security threshold, they can benefit from improved security procedures. The implementation comparison results [25] emphasise the importance of evaluating and analysing the performance of alternative encryption algorithms supplied by hardware platforms.

A trustworthy cryptographic system that exploits and utilises IoT technology is more than necessary in order to have a flexible connection between the real and virtual worlds. As a result, this paper proposes a revolutionary IoT cryptographic system with a wide range of security approaches. We provide a technique for several security levels in terms of encryption/decryption, as well as their practical application in IoTdevices, in this study. Furthermore, a detailed examination of the security levels as they relate to communication between the IoT layers of the architecture is included. The proposed cryptographic system can be further developed as an extended invited work of their preliminary publication as a more sophisticated design and powerful system; the goal could be to expand the system by incorporating other cryptographic primitives such as Public Key Cryptography, Hashing, and Digital Signatures. Future research areas could include lightweight cryptography, such as streamciphers, as well as cryptography and security systems for the sensitive sector of health and medical applications. This system should also be able to connect to many boards that use the same platform technology for data sharing and to recommend solutions to various security issues [25].

The Internet was created with the intention of allowing people to share resources. The Internet has steadily changed from a resource sharing mode to an information sharing mode as a result of recent technology advancements and a large demand for information. The content centric network (CCN) is a blank-slate Internet architecture designed to meet the demands of modern Internet usage patterns. This study provides a secure content distribution architecture for CCN based on elliptic curve cryptography and public key infrastructure (ECC-PKI). The proposed method restores the Internet's present commercial model by

separating encrypted content from its access control specifications while preserving the CCN's in-network content caching mechanism.In the proposed security architecture, content will be safely transmitted between each pair of CCN entities using ECC-based protocols. Our primary goal in developing proposed protocols is to reduce computation and communication costs while improving performance, efficiency, and security.Finally, a formal security verification using the well-known AVISPA simulator and BAN logic finds that the proposed system is secure against the existing relevant cryptographic attacks [26].

This work proposes a CCN-based ECC-based content dissemination architecture that is both efficient and safe, including ECC-based protocols for all critical interactions between entities. This method introduces a computationally efficient packet naming technique. The suggested approach not only enables mutual verification between content producers and publishers, as well as publishers and consumers, but it also ensures content integrity. According to the security analysis using BAN logic and the AVISPA simulator, as well as the performance assessment, the proposed system provides a cost-effective security solution for CCN. As a result, the proposed scheme provides a fundamental content distribution framework upon which any other business model or subscription mechanism, such as a revenue model for telephony conversations, can be built. In the suggested system, the publisher is an integral component of the content provider, and both are expected to be trustworthy. As a result, the consumer trusts the publisher as a content provider. In content delivery networks, however, authenticating the content provider whose content is given through a third-party publisher is a key challenge (CDN). These characteristics, however, are expected to represent the work's future scopes [26].

The user server mutual authentication architecture, which is based on smart cards, is well-known for ensuring secure communication over insecure networks. The authenticated user and server connect with one another over the Internet and share information. A smart card-based password-assisted two-factor authentication solution has been presented by Wang et al. They investigated their system and determined that it protects against password guessing and impersonation assaults while maintaining security and privacy. They proposed an upgraded elliptic curve cryptography (ECC)-based authentication method for the same context. Some of the appealing security attributes and features of the proposed scheme ESEAP include offline password guessing attack, no password verifier-table, smart card loss attack, anonymity, mutual authentication, replay attack, impersonation attack, server spooling attack, no clock-synchronization attack, forward secrecy, insider attack, message authentication, and provision of key agreement. A formal security analysis of the ESEAP based on a random oracle model is also included in the study. They compared ESEAP to similar protocols in the same environment and discovered that it is more efficient in terms of processing and communication [27].

Wang et alapproach. has a variety of security issues, including an off-line password guessing attack and an impersonation attack, according to the research. The paper has offered a solution by establishing an ECC-based secure and efficient mutual authentication system using smart cards. They also showed that the suggested framework offers more security and functionality than competing alternatives. In addition, they provided a formal ESEAP security proof based on a random oracle model. The proposed protocol is more efficient in terms of computing and communication cost when compared to other protocols in the same situation. As a result, the proposed protocol [27] can be implemented in a real-world

communication system.

The Internet of Things (IoT) presents a significant security concern. The purpose of this study is to develop and evaluate a dynamic IoT security system based on a generic IoT edge network in which nodes use the MQTT protocol to communicate.
This work aims to improve MQTT security by preventing data tampering, eavesdropping, and replay attacks using Elliptic Curve Cryptography (ECC), timestamps, and wake up patterns, with the purpose of conserving node energy. The findings will indicate that by tying security and energy levels together, it is possible to extend the system's lifetime [28].

The sensor and actuator nodes in a fog network exchange data using a secure MQTT protocol in this article, which presents a new dynamic IoT security architecture. The proposal encrypts MQTT payloads with ECC, adds a timestamp to the payloads, and uses lightweight node wake-up patterns to prevent Replay attacks to prevent data modification and eavesdropping. They recommended altering the key-strength of the used ECC dynamically depending on residual energy capacity to reduce encryption energy consumption, while taking care to adjust the key change frequency based on the current key-strength.Using a wake-up pattern also minimises the number of received repeated packets as well as the energy required to dump them.The suggested security system was evaluated using an event-driven simulator, which indicated that the approach increases the system lifetime (at the cost of an increase in key exchange overhead) and mitigates replay assaults by minimising energy waste associated with the dropping process.In order to reduce the amount of energy consumed, their future work will primarily focus on applying new elliptic curves and other cryptographic approaches to both fog and cloud computing environments. Furthermore, they are already working on fog computing mitigation of DoS attacks [28].

Internet-of-Things (IoT) is rapidly expanding in today's world as a result of digital transformation. Cloud computing has also grown more important for many applications in the digital era to handle massive amounts of data. When dynamically acting users access the programme, the gap between cloud data security and user privacy must be bridged as soon as possible. The authors of this paper [29] propose a Multi-Dimensional Access Control (MD-AC) technique for dynamically authorising and revoking users in the cloud who have several authorities.The proposed MD-AC paradigm was successful in restricting the power of the central authority. It also includes dynamic revocation threshold vectors, which can revoke a user at any point during the authorisation process, depending on the network threat level. The ciphertext cannot be re-encrypted or decrypted without first providing the decryption.

According to the results of the tests, Multi-Dimensional Access Control can evaluate access requests in a reasonable amount of time. Based on highly tough experimental conditions and several transactions, the average encryption and decryption times are 18ms and 10ms, respectively. The proposed MD-AC scheme has been validated and compared to current best-practice schemes. The findings show that the proposed technique is quick and resistant to a variety of well-known attacks, and that it may be used to safeguard the privacy of cloud-based IoT services.[29]

Because of Data Mining as a Service, data owners have been successfully liberated from data administration and in-house data analysis (DMaaS). The authors of this paper[30] seek to present a solution for outsourced secure collaborative data clustering by proposing the twin

concepts Cryptographic Ensembles and Global Encrypted Distance Matrices (GEDMs).

Liu's HE scheme and the Multi-User Order Preserving Encryption (MUOPE) scheme were included in the Cryptographic Ensemble, both of which offer the advantage of removing the need for data owners to participate in the clustering process.
The Cryptographic Ensemble has no negative impact on Clustering Accuracy. This study presents a general method that can be used for a variety of safe data mining applications, including data clustering.[30]

Data storage over the internet and cloud has increased dramatically in the realm of digital communication, which has resulted in data security challenges as private data has been compromised by many hackers.To safeguard the data using Fog computing, huge efforts have been made employing steganography and cryptography. Due to their relative complexity and data redundancy, video steganography makes files more secure against hacker attempts.

The author proposes a new hybrid security method (HS2) to secure fog computing in this paper[31], which combines the benefits of both cryptography and steganography. By creating a new encryption strategy that uses -blocks of linear feedback shift registers (LFSRs) coupled with an adder/subtractor to produce a strong secret key for each block end, HS2 embeds a concealed picture into a video as the host medium. To acquire the encrypted secret picture, the secret image will be XORed with the created final key using a nonlinear function.Another addition from this approach is a new steganography technology based on an enhanced discrete wavelet packet transform (DWPT) to insert the encrypted secret image into a cover movie. When applied to a fog environment, the suggested HS2 outperforms similar security measures and resists typical assaults, according to the testing results and security analysis. [31]

Airlines cargo companies do not impose a fee for last-minute cancellations of shipments in order to establish strong long-term connections with its clients. This allows them to schedule the same shipment with many cargo companies.Cargo enterprises are unable to fine-tune the proper overbooking level as a result of the high unpredictability in the quantity of cancellations, resulting in losses.

In this paper[32], the authors demonstrate how enabling computation on private consumer and company data can strengthen the overall service chain, allowing for better agreements to be established and enforced through the use of cryptographic techniques. The authors propose a query strategy based on proxy re-encryption and show how relevant data may be recovered while preserving client anonymity. In addition, this paper presents a Game Theoretic model of the use case scenario, with findings proving that it allows for more accurate cancellation rate estimation. This methodology helps to reduce uncertainty and may be used to fine-tune the level of overbooking.[32]

The Internet of Things (IoT) differs from traditional Internet-connected devices in that it is capable of doing complex tasks on its own with littleor no human intervention.However, with theintroduction of heterogeneous technology, IoT network security has become a big worry.Even as quantum computers get more powerful, cryptographic systems based on mathematical problems are no longer reliable.The authors of this paper[33] examined the

importance of post-quantum cryptography approaches in protecting IoT networks in depth.

The authors provided a full explanation of the layered architecture of IoT, as well as the accompanying problems and countermeasures, as well as a detailed overview of traditional cryptographic algorithms.To prevent quantum computer attacks, it's critical to forsake cryptographic approaches based on old mathematical issues in favour of inventing algorithms based on new mathematics techniques, which will help in the post-quantum IoT future with attack resistance.[33]

Drones in the Internet of Drones (IoD) have been widely used in a variety of industries and have shown to be quite effective in a wide range of applications. The data acquired by sensors deployed in drones faces new security and privacy risks with each technical innovation. Many writers have proposed various authentication and key agreement (AKA) mechanisms to ensure the security of transmitted data. To address key security vulnerabilities in high communication and computation cost issues in IoD, the author[35] presented a lightweight AKA technique to secure one-way hash function and bitewise XOR operations when drones and users reciprocally authenticate each other.According to this research [35], the suggestedapproach can attain AKA-security under the random oracle paradigm and withstand numerous known attacks. The proposed method outperforms the prior schemes in terms of communication and computing costs, as well as functionality. [34].

As wireless technologies such as RFID, Bluetooth, and Wi-Fi have grown more widely available, the Internet of Things (IoT) has gradually emerged in today's society. According to the National Institute of Standards and Technology, the security level of RSA is secure when it is N-bit modulus 2048 bits (NIST). As a result, the processing time for generating asymmetric keys has increased.The authors of this paper[36] proposed an efficient and non-shareable Public Key Exponent Secure Scheme (ENPKESS) that performs three steps of encryption and two stages of decryption using the Diophantine equation with RSA public keys. To provide high security in cloud systems, the Knapsack technique is utilised to encrypt the ENPKESS keys.According to the experimental results, the ENPKESS scheme allows for appropriate time computation by utilising around 0.24 periods of ESRKGS and 0.82 periods of Standard RSA. ENPKESS has a longer cypher and decipher time than other schemes, and the timing similarity shows that ENPKESS and RSA have 100% correlation, whereas ESR and RSA have 90%. This technique provides high-strength protection for confidential data while retaining a manageable key size. The proposed approach appears to be resistant to side-channel assault based on the findings obtained.[35]

Table 3
Advantages and Disadvantages of Certain Investigations onCryptography Techniques and Internet of Things Applications

Reference	Method	Advantage	Disadvantage
[1]	Proof-based verifiable computing Replication-based Verifiable Computing	When both the client and the cloud are honest, the cost of using smart contracts is almost non-existent.	
[2]	a combination of the Whale Optimization	In every regard, including temperature, load, delay,	

	Algorithm and the Moth Flame Optimization (MFO)	energy, total number of alive nodes, and cost function, the proposed model surpasses other models.	
[3]	Shodan, Packet sniffing applications and network mapping tools	Exercise obscurity and limit the availability of assets to authorised persons as part of reducing the attack surface.	
[4]	LAM-CIoT	When compared to closely related authentication systems, LAM-CIoToffers provides higher security and has lower communication and computation overheads.	
[5]	Using binary Edward curves, an FPGA-based acceleration engine for main ECC operations has been developed.	The design is small and broad, requiring less than 1400 Virtex-5 FPGA slices to provide 128-bit security.	Despite the fact that it is not well suited for high-performance applications, it can be highly enticing in situations where space is limited.
[6]	LoRa+	LoRa+ increases ED-GW connection while reducing interference and collisions. In a region with high ED density, it also allows LoRa network operators to cut the number of GWs by up to 80%, resulting in significant cost savings.	
[7]	Based on the Multivariate Cubic (MC) issue, a framework for digital signatures has been developed.	The signature size in their system is less than all other MPKC-based signature schemes under the same security assumptions.	
[8]	a cloud-based digital picture locker with secure user identification and a new image cryptosystem to keep user photos private	Under the same security assumptions, the signature size of their system is smaller than all other MPKC-based signature methods.	
[9]	The CB-PBS (certificate-based	The CB-PBS signature technique proposed is the	The construction of a pairing-free short

	proxy blind signature) technique	most efficient and quickest.	CB-PBS system is an open problem due to the high cost of pairing.
[10]	LB-2PAKA protocol	In the random oracle model, it provides provable security. The LB-2PAKA protocol will be more appropriate than standard 2PAKA protocols for many Internet-based applications in post-quantum contexts.	
[11]	VCC authentication architecture based on elliptic curve cryptography (ECC)	The suggested framework fulfils all desired security features while also facilitating effective communication.	
[12]	the chirp spectrum modulation technique was used to analyse the system level outage of a single LoRa Gateway.	When the conditional outage probability is compared to the unconditional outage probability, it is discovered that the second outage probability has a greater impact on both the outage and coverage likelihood. The study also discovered that adding other LoRa gateways in the same geographical region reduces the LoRa Gateway's overall performance even further.	
[13]	data transmission that is secure Using Modified Elliptic Curve Cryptography (MECC) and Deep Learning Modified Neural Networks, early detection of anti-forensic attacks in the cloud is possible (DLMNN)	In terms of precision, f-measure, recall, accuracy, sensitivity, and specificity in the detection of attacks, DLMNN outperforms prior systems such as DLNN and KNN. MECC has a security score of 96 percent, compared to 90 percent for the old ECC and 87.5 percent for the existing RSA-based approach.	

[14]	Schmidt-Samoa Cryptography (SKMA-SC) method with Multi-Factor Authentication with Suppressed K-Anonymity	The performance of the SKMA-SC approach was assessed using computational complexity (CC) and privacy-preserving rate (PPR) with a variety of clients and cloud data, with promising findings.	
[15]	redundant energy consumption laxity based (RECLB) algorithm	Perform each application process in a redundant and energy-efficient manner on many virtual computers.	
[16]	twin Peaks	By extending the naming method, TwinPeaks can be used in IoT contexts.	Twinpeaks' public key is based on both its IP address and domain name, therefore impersonation by a single organisation (such as a DNS or key server) is impossible.
[17]	WoT Store	In a small-case testbed, they first demonstrated Thing discovery and the ability to run WoT applications that orchestrate the operations of multiple, heterogeneous Wireless Sensor Networks (WSNs), and then they demonstrated the platform's scalability and ability to aggregate and visualise data in a mixed real/simulated large-scale crowdsensing scenario.	
[18]	a centralised inconspicuous IoT-based device-type invariant fall detection and rescue system for real-time monitoring of a big population	The proposed approach obtained accuracy of 99.7%, sensitivity of 96.3 percent, and specificity of 99.6%. The designed system is extremely fast, with a response time of about 190 milliseconds.	
[19]	In the standard	The user's privacy is	

	approach, attribute-based encryption is decentralised.	completely protected. Both identity–anonymity and attribute–anonymity are secured against untrusted attribute authorities during the creation of private keys.	
[20]	Extension of the authentication technique for safe control of devices from powerful cloud servers	The system is secure and can be used on small embedded devices.	
[21]	CWD-WPT charging systems on a VANET network in a cloud and fog computing environment	gives better security and safety analysis results while avoiding the centralization issues that come with combining fog and cloud computing in a cloud environment. As a result of this combination, the computational processing of processes in the devices is distributed more uniformly, and communication latency is reduced.	
[22]	CAPODAZ (containerized authorization and policy-driven architecture) is a microservices-based architecture.	In terms of latency, throughput, and successful queries, there is a significant improvement. The best CAPODAZ performance was shown in the most realistic situation (Poisson), in which the load was irregularly distributed in time and requests arrived at a rapid rate.	
[23]	SCF-CLSPE scheme	When compared to Rhee et al.'s technique, it has a high encryption efficiency.	The proposed technique performs somewhat worse in the test phase than Lu et al.'s scheme.
[24]	Certificateless Aggregate Cryptography Signature Scheme	The TPA side of the system is more efficient, as it is lighter and better suited to cloud-based HER.	

	using Elliptical Curve (EC-ACS)		
[25]	IoT cryptographic system	It offers a vast number of security schemes.	
[26]	elliptic curve cryptography-based public key infrastructure provides a secure content dissemination architecture for CCN (ECC-PKI).	The proposed technique is resistant to known cryptographic vulnerabilities and provides CCN with a low-cost security solution.	
[27]	ESEAP	In terms of computation and communication expenses, ESEAP is more efficient, and the suggested protocol is a real-world communication system application.	
[28]	new dynamic IoT security system through (MQTT) protocol	Proposal extends the system lifetime (at the cost of an increase in key exchange overhead) and mitigates replay assaults by minimising energy waste associated with the dropping procedure.	
[29]	Multi-Dimensional Access Control (MD-AC) scheme	The suggested approach is quick and secure against a variety of well-known attacks, and it may be used to protect the privacy of IoT services in the cloud.	
[30]	Cryptographic Ensembles and Global Encrypted Distance Matrices (GEDMs).	The suggested approach is quick and secure against a variety of well-known attacks, and it may be used to protect the privacy of IoT services in the cloud.	
[31]	hybrid security strategy (HS^2)	Based on the experimental results and security analyses completed, HS^2 outperforms similar security measures and resists typical assaults when applied to the fog environment.	
[32]	based on proxy re-	It is proposed a theoretical	

	encryption query system	model of the use case scenario, with findings proving that it allows for more accurate cancellation rate prediction. This strategy can be used to fine-tune the level of overbooking and reduce uncertainty.	
[33]	post-quantum cryptographic techniques for securing IoT networks	In the post-quantum IoT future, it aids in the resistance against attacks.	
[34]	lightweight AKA scheme	Under the random oracle model, the suggested technique can achieve AKA-security and withstand many known attacks. The proposed method outperforms the prior schemes in terms of communication and computing costs, as well as functionality.	
[35]	ENPKESS (Efficient and Non-Shareable Public Key Exponent Secure Scheme) is a mechanism that is both efficient and non-shareable.	The ENPKESS system uses 0.24 periods of ESRKGS and 0.82 periods of Standard RSA for precise time computation. ENPKESS has a longer cypher and decipher time than other schemes, and the temporal similarity shows that ENPKESS and RSA have a 100% correlation, while ESR and RSA have a 90% correlation. This technique provides high-strength protection for confidential data while retaining a manageable key size. Based on the data, the proposed technique appears to be resistant	

		against side-channel attack.	

Table 3 shows the advantages and disadvantages of certain investigations on Cryptographic techniques and Internet of Things applications.

This paper has looked at what cryptography is and how it can be used to encrypt and decode data.To safeguard data and prevent it from being hacked, cryptography is utilised in all fields.For example, password security, banking transaction authentication, and so on.Various new cryptographic algorithms are invented and cracked every day; as a result, it is critical to be aware of computer risks at all times and to take precautions to avoid them as much as possible.

Users can accomplish deeper automation, analysis, and integration inside a system with IoT solutions. They increase the range and precision of these domains. For sensing, networking, and robotics, the Internet of Things employs both existing and emerging technology.

The Internet of Things capitalises on recent software advancements, lower hardware prices, and modern technology attitudes. Its innovative and sophisticated features result in substantial changes in how products, goods, and services are delivered, as well as the social, economic, and political consequences of those changes.

2. CONCLUSION

In this paper, Certain Investigations on Cryptography Techniques and Internet of Things Applications are been proposed. In cryptographic techniques, Verifiable computing based on proofs and verifiable computing based on replication, FPGA, Multivariate Cubic MC problem, image cryptosystem, CB-PBS scheme, LB-2PAKA protocol, MECC and DLMNN, SKMA-SC technique, EC-ACS Scheme, IoT cryptographic system, ECC-PKI, ESEAP, GEDMs, hybrid security strategy HS^2, query system based on proxy re-encryption, post-quantum cryptography approaches, such as a hybrid Whale Optimization Algorithm-Moth Flame Optimization, for safeguarding IoT networks and IoT applications (MFO), Shodan, Packet sniffing applications and network mapping tools, LAM-CIoT, LoRa+, The chirp spectrum modulation method is used in the LoRa Gateway, RECLB algorithm, twin Peaks, WoT Store, a centralised, unobtrusive IoT-based device-type invariant fall detection and rescue system for real-time population monitoring, decentralized attribute-based encryption in the standard model, authentication scheme, CWD-WPT charging systems on a VANET network in a cloud and fog computing environment, CAPODAZ, SCF-CLSPE scheme, IoT cryptographic system, MQTT, Multi-Dimensional Access Control (MD-AC) scheme, protecting IoT networks with post-quantum cryptography techniques lightweight AKA scheme and ENPKESS method. Both Cryptographic Techniques and Internet of Things provide good results in terms of precision, sensitivity,f-measure, recall, accuracy and specificity and provides high efficiency and offers a vast number of security schemes.

FUTURE SCOPE

Researchers are working on quantum-safe encryption, according to Moody, to counteract attempts to crack encrypted data with quantum computers. Current cryptography is concerned with discovering and evaluating methods that prohibit third parties or the general

public from accessing private messages. Data secrecy, data integrity, authentication, and non-repudiation are all significant components of modern encryption.

The future of IoT is essentially endless, thanks to technical improvements and customers' desire to link electronics such as mobile phones with domestic machines. People and devices on all platforms can now be connected thanks to a networking and connectivity protocol.Furthermore, there is a tremendous amount of data being transferred from one gadget to the next.To keep up with demand, another major problem will need to be addressed: security.Individually, IoT presents significant professional chances that must be taken advantage of.However, we must possess the requisite talent, which will serve as a crucial distinction.

3. REFERENCES

[1] M. R. Dorsala, V. N. Sastry, and S. Chapram, "Fair payments for verifiable cloud services using smart contracts," *Computers& Security*, vol. 90, p. 101712, March. 2020, doi: 10.1016/j.cose.2019.101712.

[2] P. K. R. Maddikunta, T. R. Gadekallu, R. Kaluri, G. Srivastava, R. M. Parizi, and M. S. Khan, "Green communication in IoT networks using a hybrid optimization algorithm," *Computer Communications*, vol. 159, pp. 97–107, June. 2020, doi: 10.1016/j.comcom.2020.05.020.

[3] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT network," *Internet of Things*, vol. 9, p. 100162, March. 2020, doi: 10.1016/j.iot.2020.100162.

[4] M.Wazid, A. K. Das, V. Bhat K, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *Journal of Network and Computer Applications*, vol. 150, p. 102496, Jan. 2020, doi: 10.1016/j.jnca.2019.102496.

[5] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight elliptic curve cryptography accelerator for internet of things applications," *Ad Hoc Networks*, vol. 103, p. 102159, June. 2020, doi: 10.1016/j.adhoc.2020.102159.

[6] H.Mroue et al., "LoRa+: An extension of LoRaWAN protocol to reduce infrastructure costs by improving the Quality of Service," *Internet of Things*, vol. 9, p. 100176, March. 2020, doi: 10.1016/j.iot.2020.100176.

[7] N.Kundu, S. K. Debnath, D. Mishra, and T. Choudhury, "Post-quantum digital signature scheme based on multivariate cubic problem," *Journal of Information Security and Applications*, vol. 53, p. 102512, Aug. 2020, doi: 10.1016/j.jisa.2020.102512.

[8] V. R. Falmari and M. Brindha, "Privacy preserving cloud based secure digital locker using Paillier based difference function and chaos based cryptosystem," *Journal of Information Security and Applications*, vol. 53, p. 102513, Aug. 2020, doi: 10.1016/j.jisa.2020.102513.

[9] G. K. Verma, B. B. Singh, and H. Singh, "Provably secure certificate-based proxy blind signature scheme from pairings," *Information Sciences*, vol. 468, pp. 1–13, Nov. 2018, doi: 10.1016/j.ins.2018.08.031.

[10] S. H. Islam, "Provably secure two-party authenticated key agreement protocol for post-quantum environments," *Journal of Information Security and Applications*, vol. 52, p.

102468, June. 2020, doi: 10.1016/j.jisa.2020.102468.
[11] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," *Vehicular Communications*, vol. 22, p. 100213, April. 2020, doi: 10.1016/j.vehcom.2019.100213.
[12] N.Aftab, S. A. R. Zaidi, and D. McLernon, "Scalability analysis of multiple LoRa gateways using stochastic geometry," *Internet of Things*, vol. 9, p. 100132, March. 2020, doi: 10.1016/j.iot.2019.100132.
[13] D. R. Rani and G. Geethakumari, "Secure data transmission and detection of anti-forensic attacks in cloud environment using MECC and DLMNN," *Computer Communications*, vol. 150, pp. 799–810, Jan. 2020, doi: 10.1016/j.comcom.2019.11.048.
[14] K.MohanaPrabha and P. VidhyaSaraswathi, "Suppressed K-Anonymity Multi-Factor Authentication Based Schmidt-Samoa Cryptography for privacy preserved data access in cloud computing," *Computer Communications*, vol. 158, pp. 85–94, May 2020, doi: 10.1016/j.comcom.2020.04.057.
[15] T.Enokido and M. Takizawa, "The Redundant Energy Consumption Laxity Based Algorithm to Perform Computation Processes for IoT Services," *Internet of Things*, vol. 9, p. 100165, March. 2020, doi: 10.1016/j.iot.2020.100165.
[16] E. Cho et al., "TwinPeaks: An approach for certificateless public key distribution for the internet and internet of things," *Computer Networks*, vol. 175, p. 107268, July. 2020, doi: 10.1016/j.comnet.2020.107268.
[17] L.Sciullo, L. Gigli, A. Trotta, and M. D. Felice, "WoT Store: Managing resources and applications on the web of things," *Internet of Things*, vol. 9, p. 100164, March. 2020, doi: 10.1016/j.iot.2020.100164.
[18] S.Nooruddin, Md. Milon Islam, and F. A. Sharna, "An IoT based device-type invariant fall detection system," *Internet of Things*, vol. 9, p. 100130, March. 2020, doi: 10.1016/j.iot.2019.100130.
[19] H.Nasiraee and M. Ashouri-Talouki, "Anonymous decentralized attribute-based access control for cloud-assisted IoT," *Future Generation Computer Systems*, vol. 110, pp. 45–56, Sep. 2020, doi: 10.1016/j.future.2020.04.011.
[20] T. K. Dang, C. D. M. Pham, and T. L. P. Nguyen, "A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities," *Sustainable Cities and Society*, vol. 56, p. 102097, May 2020, doi: 10.1016/j.scs.2020.102097.
[21] L. F. A. Roman and P. R. L. Gondim, "Authentication protocol in CTNs for a CWD-WPT charging system in a cloud environment," *Ad Hoc Networks*, vol. 97, p. 102004, Feb. 2020, doi: 10.1016/j.adhoc.2019.102004.
[22] D.Kallergis, Z. Garofalaki, G. Katsikogiannis, and C. Douligeris, "CAPODAZ: A containerisedauthorisation and policy-driven architecture using microservices," *Ad Hoc Networks*, vol. 104, p. 102153, July. 2020, doi: 10.1016/j.adhoc.2020.102153.
[23] M. Ma, D. He, S. Fan, and D. Feng, "Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare," *Journal of Information Security and Applications*, vol. 50, p. 102429, Feb. 2020, doi: 10.1016/j.jisa.2019.102429.
[24] T.Benil and J. Jasper, "Cloud based security on outsourcing usingblockchain in E-health systems," *Computer Networks*, vol. 178, p. 107344, Sep. 2020, doi: 10.1016/j.comnet.2020.107344.
[25] P.Panagiotou, N. Sklavos, E. Darra, and I. D. Zaharakis, "Cryptographic system for data

applications, in the context of internet of things," *Microprocessors and Microsystems*, vol. 72, p. 102921, Feb. 2020, doi: 10.1016/j.micpro.2019.102921.

[26] S.Adhikari, S. Ray, M. S. Obaidat, and G. P. Biswas, "Efficient and secure content dissemination architecture for content centric network using ECC-based public key infrastructure," *Computer Communications*, vol. 157, pp. 187–203, May 2020, doi: 10.1016/j.comcom.2020.04.024.

[27] A.Kumari, S. Jangirala, M. Y. Abbasi, V. Kumar, and M. Alam, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," *Journal of Information Security and Applications*, vol. 51, p. 102443, April. 2020, doi: 10.1016/j.jisa.2019.102443.

[28] F. De Rango, G. Potrino, M. Tropea, and P. Fazio, "Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks," *Pervasive and Mobile Computing*, vol. 61, p. 101105, Jan. 2020, doi: 10.1016/j.pmcj.2019.101105.

[29] K.Riad, T. Huang, and L. Ke, "A dynamic and hierarchical access control for IoT in multi-authority cloud storage," *Journal of Network and Computer Applications*, vol. 160, p. 102633, June. 2020, doi: 10.1016/j.jnca.2020.102633.

[30] N.Almutairi, F. Coenen, and K. Dures, "A Cryptographic Ensemble for secure third party data analysis: Collaborative data clustering without data owner participation," *Data & Knowledge Engineering*, vol. 126, p. 101734, March. 2020, doi: 10.1016/j.datak.2019.101734.

[31] S. A. Hussein, A. I. Saleh, H. E.-D. Mostafa, and M. I. Obaya, "RETRACTED: A hybrid security strategy (HS2) for reliable video streaming in fog computing," *Journal of Information Security and Applications*, vol. 51, p. 102412, April. 2020, doi: 10.1016/j.jisa.2019.102412.

[32] S.Cimato, G. Gianini, M. Sepehri, R. Asal, and E. Damiani, "A cryptographic cloud-based approach for the mitigation of the airline cargo cancellation problem," *Journal of Information Security and Applications*, vol. 51, p. 102462, April. 2020, doi: 10.1016/j.jisa.2020.102462.

[33] A.Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things*, vol. 9, p. 100174, March. 2020, doi: 10.1016/j.iot.2020.100174.

[34] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Computer Communications*, vol. 154, pp. 455–464, March. 2020, doi: 10.1016/j.comcom.2020.02.067.

[35] C.Thirumalai, S. Mohan, and G. Srivastava, "An efficient public key secure scheme for cloud and IoT security," *Computer Communications*, vol. 150, pp. 634–643, Jan. 2020, doi: 10.1016/j.comcom.2019.12.015.

[36] L. Ogiela, M. R. Ogiela and U. Ogiela, "Cognitive information systems in secure information management and personalized cryptography," *2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS)*, 2014, pp. 1152-1157, doi: 10.1109/SCIS-ISIS.2014.7044798.

[37] J. Perdigues, "ESA studies and future trends in quantum cryptography for space systems," *2005 The IEE Seminar on Quantum Cryptography: Secure Communications for Business (Ref. No. 2005/11310)*, 2005, pp. 0_17-4/20, doi: 10.1049/ic:20050579.

[38] M. A. Latif, M. B. Ahmad and M. K. Khan, "A Review on Key Management and Lightweight Cryptography for IoT," *2020 Global Conference on Wireless and Optical*

Technologies (GCWOT), 2020, pp. 1-7, doi: 10.1109/GCWOT49901.2020.9391613.

[39] P. S. Lakshmi and G. Murali, "Comparison of classical and quantum cryptography using QKD simulator," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2017, pp. 3543-3547, doi: 10.1109/ICECDS.2017.8390120.

[40] E. Atar, O. K. Ersoy and L. Özyılmaz, "Character/text data compression and encryption by compressive sensing and hybrid cryptography," *2016 24th Signal Processing and Communication Application Conference (SIU)*, 2016, pp. 365-368, doi: 10.1109/SIU.2016.7495753.

[41] C. Lee and A. Fumagalli, "Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks," *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 24-28, doi: 10.1109/WF-IoT.2019.8767227.

[42] S. Ziegler, S. Nikoletsea, S. Krco, J. Rolim and J. Fernandes, "Internet of Things and crowd sourcing - a paradigm change for the research on the Internet of Things," *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 395-399, doi: 10.1109/WF-IoT.2015.7389087.

[43] D. Vergnaud, "Comment on "Efficient and Secure Outsourcing Scheme for RSA Decryption in Internet of Things"," in *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11327-11329, Nov. 2020, doi: 10.1109/JIOT.2020.3004346.

[44] D. Keng and S. G. M. Koo, "Spatial Standards for Internet of Things," *2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*, 2014, pp. 284-287, doi: 10.1109/iThings.2014.50.

[45] B. Xu, J. Zheng and Q. Wang, "Analysis and Design of Real-Time Micro-Environment Parameter Monitoring System Based on Internet of Things," *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016, pp. 368-371, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.87.