Global Scientific JOURNALS

GSJ: Volume 12, Issue 2, February 2024, Online: ISSN 2320-9186

www.globalscientificjournal.com

SECURING THE INTERNET OF THINGS: An Exploration of IoT Security Through Advanced Encryption

Atalor Osaroboh Daniel, Courage Obajaja

KeyWords

Security, Internet of Things, Cryptography, Internet of everything, Microsoft Message Queue, Network devices.

Abstract

The Internet of Things (IoT) encompasses a global network of interconnected devices utilizing established communication standards. It involves the exchange of information wirelessly among embedded computing devices connected to the internet. Network security solutions must be tailored to the unique challenges posed by IoT, requiring security measures similar to those for traditional systems. Key security considerations include trust management, authorization, authentication, identity, access control, network security, standardization, and interoperability. The significance of addressing these issues is heightened in the context of increased attack vectors and routes, especially when dealing with the exchange of personal data.

The proposed study aims to address critical security concerns in the Internet of Things (IoT) landscape by implementing advanced encryption techniques. IoT has revolutionized various sectors, offering unprecedented connectivity and functionality. However, this interconnectedness brings forth significant security challenges, necessitating robust measures to safeguard sensitive information.

The methodology involves modeling two IoT devices using the MQTT protocol for communication, with a particular emphasis on securing mission-critical data through end-to-end AES encryption. The research will employ Microsoft Message Queuing Protocol (MSMQ) as an instance of Advanced Message Queuing Protocol (AMQP), ensuring secure communication between the simulated IoT devices. Furthermore, the study acknowledges the significance of the IoT ecosystem in diverse domains, such as healthcare, productivity enhancement, and smart infrastructure. By reviewing the existing literature, the research aims to identify gaps in current security measures and contribute to the body of knowledge regarding IoT security and encryption.

The anticipated outcomes include a refined understanding of encryption techniques applicable to IoT, enhanced security measures for IoT devices, and potential solutions to mitigate security risks. The study's findings will benefit organizations, users, and stakeholders involved in IoT, fostering a more secure and resilient IoT environment.

INTRODUCTION

1.1 Background to the Study

The proliferation of interconnected devices in the digital landscape, commonly referred to as the Internet of Things (IoT), has ushered in unprecedented convenience and efficiency across various sectors. However, this interconnectedness has also given rise to significant concerns, particularly in the realm of security. As the volume of sensitive data exchanged between IoT devices continues to escalate, the need for robust security measures becomes paramount. Cryptography emerges as a key player in fortifying the security posture of IoT devices, offering a reliable means to safeguard data confidentiality, integrity, and authentication (Chen, & Liyanage, 2019).

Two fundamental approaches in cryptographic solutions are symmetric and asymmetric algorithms. Symmetric algorithms employ a single key for encryption and decryption, ensuring the confidentiality and integrity of data. On the other hand, asymmetric algorithms utilize a pair of keys, public and private, enabling a more versatile set of security features, including confidentiality, authentication, and integrity. Despite the benefits of IoT, it is open to security breaches. Some concerns can affect both the physical properties and the life of the individual.

It has the potential to alter the planet even over the web has done. Connecting electronic objects into the digital network has been ongoing for a very long term. This success is due in part to radio frequency identification and wireless sensor network technologies. The Internet of Things (IoT) combines several devices with numerous platforms, computing capabilities, and functions. The heterogeneity of the network and the ubiquity of IoT devices place increased demands on security and privacy protection (Ramaswamy, 2015).

IoT provides a network infrastructure with interoperable communication protocols and software tools to enable the connectivity to the internet for handheld smart devices (Liyanage, and Chen, 2018) such as smartphones, personal digital assistants (PDA) and tabs), good home equipment (smart TV, AC, intelligent lighting systems, good refrigerator, etc.), vehicles, and sensory acquisition systems). However, the improved connectivity and accessibility of devices present major concerns for the security of all the parties connected to the network regardless of whether they are humans or machines.

The Internet of Things, like any fast-evolving technology, has several security issues. The greater the number of devices linked to the network, the greater the risk of attackers gaining and exploiting others (Aljarah, et al, 2020). As IoT systems are increasingly entrusted with sensing and managing highly complex ecosystems, concerns about the security and reliability of data transmitted to and from IoT devices are quickly becoming a major concern (Alaba, & Othman, 2017).

As the number of linked items grows, so will the number of breaches the system is exposed to. These IoT platforms include sensitive or proprietary content that could be leaked (Temirbekova and Pyrkova, 2020). Also, the growth of connected devices will continue to increase in hundreds of millions. This shows that society will increasingly rely on such devices in business and other personal-related dealings. The Internet has become second nature to billions of people already for it allows enormous gains in productivity, efficiency, and communication; however, security loopholes inherent in it can endanger business and personal lives. Creating a channel whereby hackers or third parties cannot have access to personal messages (Shankar, and Jenifer, 2017) sent out through IoT devices.

According to Baijian (2017), the primary factor for communication problems is the absence of incapable security measures to hold against attacks during internet connections. In addition, addressing these security flaws necessitates the increased use of cryptography to secure communication between IoT devices. What this implies is that the work must continue to ensure that cryptography is robust to defend against intrusion. Simultaneously, they must be efficacious sufficiently to be used on devices that are disabled (Muneer, et al, 2020).

The use of information systems has long been associated with concerns about user security and privacy (IS). The confidentiality, integrity, and availability of an asset are all protected from unauthorized disclosure, alteration, destruction, or interruption (Sattarova et al., 2000). Businesses have saved money on security in the long term by investing in high-end situations. The author discovered that "the more vulnerable the data is, the more money will be spent on information security." The higher the cost of vulnerability prevention, the riskier the project. According to the Ponemon (2015) report, the average cost of a data breach to a company increased from $376,000,000 in 2014 to $534,645,500 in 2015.

In addressing security concerns, cryptographic solutions, including both symmetric and asymmetric algorithms, play a crucial role. Symmetric algorithms utilize a single key for both encryption and decryption, ensuring data confidentiality and integrity. Asymmetric algorithms, on the other hand, involve the use of two keys, public and private, providing features like confidentiality, authentication, and integrity.

Encryption serves as a vital means to protect data stored on devices, during transit, and in the cloud. Its widespread adoption by individuals and organizations contributes to enhanced security and safety in society, preventing crimes such as data theft. The use of asymmetric algorithms, where the sender encrypts data with the receiver's public key and maintains authentication through private key encryption, exemplifies the multifaceted advantages of cryptographic techniques. Hence, the study addresses the imperative need for robust cryptographic solutions to safeguard data and systems in an increasingly interconnected and data-driven world.

1.2 Statement of the Problem

A heterogeneous system such as IoT creates a deployment problem. This heterogeneity poses many security challenges. On the other hand, the extent systems are vulnerable to infiltration from third parties has also increased. The complexity of cloud IoT architecture design, security architecture, and their unique deployment models make security a challenge for computing systems. Attacks on IoT can be physical internetwork and encryption programs. The effect of these attacks can be seen in the 2016 devastating attacks on the network and finance of companies by DNS. The attack has shown that more research is needed in IoT security systems (Lakshmi, and Srikanh, 2018).

Previous research on IoT has not provided entirely comprehensive answers to security problems. All the surveys conducted have undoubtedly emphasized one similar element, namely the restricted environment and rapid expansion of IoT technology (Ritu, Sanjay, 2014). Despite these efforts, no substantial advances in security and privacy are apparent within the IoT sector, particularly inside cloud IoT systems, and there are numerous outstanding problems to overcome (Narender, and Anita, 2014). Despite these efforts, no substantial advances in security and privacy are apparent within the IoT sector, particularly inside cloud IoT systems, and there are numerous outstanding problems to overcome (Narender, and Anita, 2014).

Version (2016) discovered that there were over 100,000 records in 2016, with 3,141 confirmed breaches. Hacker groups such as Anonymous have caused major firms to lose millions of dollars as a result of their operations. The actual cost was 126.875 billion dollars (Sandra, 2012). Cybercrime is the single most serious threat to national security, outranking all other forms of organized crime and general fraud combined (Armin, and Thompson, 2015). According to surveys conducted in recent years, Bugs and issues have been accumulating at an alarming rate (Schat, and Angelis, 2016). The possibility or danger that a device is exposed to harm that would result, and the time and resources required to accomplish a degree of protection are all factors in determining a device's security (Mulani, & Pingle, 2016). Organizations should focus on and raise awareness of information security concerns.

IoT devices can be secured with encryption but can still suffer from a brute-force attack. A wrongdoer or agency that doesn't grasp how it works might create measures abundant and computer program to hack into the system. This is why encoding needs to be extraordinarily robust and complicated. Another problem with attempting to secure a device is that making a device most important doesn’t necessarily mean it is the best approach or best or most practical approach. Increasing the key size or iterating over the algorithm could make algorithms much safer, but these ultra-secure algorithms would be extremely sluggish and resource-intensive, making them practically unworkable. Algorithms that are recommended aim to reach the optimal balance between security and usefulness.

In the encryption world, some elements are becoming outdated. 3DES is still in use but it looks might be retired shortly. Utilizing science New Year's Ev algorithm, going secret writing with different government agency steerage results in 3DES. Nowadays, many researchers have proposed many encryption and decryption algorithms: Rivest Shamir Adleman, etc. However, the major algorithms proposed had drawbacks such as unreliability and requiring considerable amounts of time to increase the delay of packets for the communication channel, which impedes the communication process.

1.3 Objectives of this Study

The main aim of this study is to develop a strong security framework for Internet of Things (IoT) devices, incorporating advanced encryption techniques.

This involves designing and implementing an encryption-decryption system utilizing asymmetric encryption specifically for password protection in IoT communication. The study further intends to assess the performance and effectiveness of the implemented security framework through thorough testing, ensuring its reliability and robustness in safeguarding IoT devices from potential threats.

1.4 Expected Contribution to Knowledge

The anticipated contribution to knowledge lies in the study's relevance to organizations and users of cloud IoT devices by focusing on securing these devices through encryption algorithms. The research addresses crucial concerns related to data availability, vulnerability, confidentiality, integrity, and the overall economic well-being of the public. The significance of these aspects stems from their potential impact on various sectors. The research aims to offer alternative security measures, promoting more efficient usage and enhancing the functioning of individuals, state institutions, and public administration.

LITERATURE REVIEW

The literature review in this study is a crucial exploration of existing knowledge on IoT security and encryption. It systematically examines a broad range of academic works to establish a robust foundation, covering historical context, theoretical frameworks, methodologies, and key findings. Apart from providing insights, the review critically assesses the field, identifying gaps and limitations that shape the research questions and objectives. This comprehensive examination sets the stage for the original contribution this study intends to make to the current body of knowledge in IoT security and encryption.

2.1 Internet of Things Security

The Internet of Things (IoT) works to provide various services by linking people on the one hand with sensors IT components, and actuators on the other hand, these services are widely used. Also, the number of connected devices on the Internet of Things is increasing tremendously. In 2015, nearly 15 billion devices were connected, and in 2019 they reached nearly 26 billion, and the number may reach about 75 billion devices by 2025, and the Internet of Things market around the world has doubled since 2016, and forecasts estimate. Whereby 2020 it could reach about $ 457 billion. With advances in communication technology, it is now feasible to send communications between conversing parties in a short period. Intruders must be kept out of the communications' substance. As a result, security is not only necessary but also a required feature of IoT. (Katsikas, 2018). Universal rules are projected to deal with security issues since security is more than just a technological issue; it is also a matter of awareness, mentality, people, and technique (Schaffers, 2019).

The Internet of Things (IoT) allows devices to communicate with one another. It is extensively used in industrial production and social applications, as well as a nice home, healthcare, and industrial automation. While providing unparalleled convenience, accessibility, and efficiency, IoT has recently posed serious security and privacy risks (Zhou, Jia, Peng, Zhang, & Liu, 2019).

The Internet of Things (IoT) refers to a new generation of technological gadgets. In the most basic sense, they are ordinary items that connect and interact over the internet. There are more things linked to the internet than humans in the world today (Evans, 2011). The term "Internet of Things" first appeared in a highly technical study by ITU (2005). IoT devices are commonly referred to as "smart gadgets," and they have a wide range of purposes and functionality (Leo & Battisti et al., 2014). Everything known as real has been turned into virtual reality as a result of IoT, which means we're all locatable and available via the internet. The Internet of Things (IoT) allows anything, anyone, or any service to be connected to a computer (Desai, 2016). Furniture, automobiles, and apparel are all good examples. All IoT devices must connect to the Internet (Revell, 2013). For years, some people have understood the word "Internet of Things (IoT)" in various ways (Ashton, 2009). According to Inerva, the Internet of Things identified gadgets and changed the state of the 'Thing' by locating and detecting a unique identification (IEEE, 2015). This definition is widely used since it is brief and unambiguous.

It is difficult to provide security in IoT devices because IoT designs must deal with many devices and different operations (Roman et al., 2013). IoT, by definition, raises security concerns. According to Leo (2014), ubiquitous sensors will be able to interact and process independently, increasing the devices' vulnerability to a cyber-attack. According to Roman (2013), when world property ("access anybody") and accessibility ("access anyway, anytime") become fundamental characteristics of cloud IoT, the number of attack routes available to malevolent attackers might skyrocket.

Everyday gadgets pose additional security concerns, and the IoT has the potential to disseminate those dangers considerably more widely than the Internet has yet (Atzori, 2010). Rose (2015) supports this viewpoint by stating that the linked nature of IoT devices implies that any poorly protected item that is connected can influence the security and resilience of the internet globally. IoT devices, in general, have limited resources, which presents problems, especially given that IoT sensors have minimal resources but require "cryptographic primitives and security protocols" (Skarmeta, and Moreno, 2013). This makes achieving high levels of security extremely challenging.

The user interface of IoT devices is restricted; many devices lack keyboards for entering passwords or even screen displays. This implies that passwords have become a weak security link in these devices since many have "default" admin passwords, weak passwords, and unencrypted data is being transmitted between devices and open ports (Desai, 2016). The use of default passwords on devices, which users are not obliged to alter when setting them up, is a widespread concern. One website claimed to have discovered 73,000 cameras that were accessible through the internet using a known default password (Soulskill, 2014).

Abie (2012) describes data integrity as a significant concern with IoT, which includes authentication, access control, and secure connectivity. Encryption is commonly used to make wireless communication more secure on today's internet. Encryption is also regarded as critical to maintaining information security on the Internet of Things (Whitmore et al., 2015). However, for IoT devices to be encrypted, algorithms must be made more effective and energy-saving, and efficient key distribution systems must be implemented (Bandyopadhyay et al., 2011).

2.2 Cryptography

Cryptography is essential for network security. The goal of cryptography is to keep transmitted data from being read and understood by anybody other than the intended receiver (Nandhini & Vanitha, 2017). Unauthorized individuals will never browse enciphered communications in general.

When communicating via an untrusted channel, such as the Internet, cryptography is essential. According to Rivest, cryptography is just "communication in the presence of adversaries." Access control, digital signatures, e-mail security, password authentication, data integrity checks, digital evidence gathering, and copyright protection are only a few of the applications for modern cryptographic approaches (Tripathi, and Sanjay, 2014).

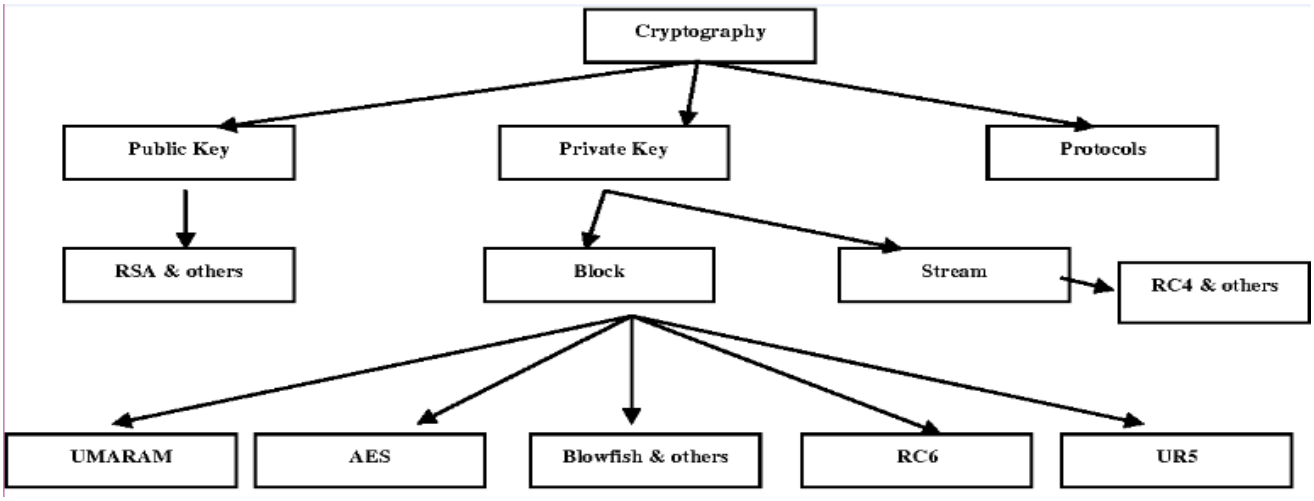


Figure 2.1 Cryptography processes (Shankar & Jenifer, 2017).

Encryption is a technique converting data into ciphertext using a cipher or encryption algorithm, ensuring security. The process involves changing plaintext into ciphertext with a key. Advanced Encryption Standard (AES) is a highly secure and fast encryption system, widely used in messaging apps like VeraCrypt, WhatsApp, Signal, WinZip, and various technologies, driven by the imperative to meet security regulations (Abd Zaid & Hassan, 2019).

Intruders should be kept out of the channel. Figure I depicts how the World Health Organization scans, inserts, deletes, or modifies communications. The transmission of a message is accomplished using an encryption function E, which transforms the message or plaintext into ciphertext using the key. The receiver does the opposite procedure, recovering the plaintext from the ciphertext using the decryption function and a decryption key (Priyanka, 2014). The main key is previously distributed through a secure channel, such as Messenger.

Normally, encoding and cryptography work, but not the key, which is revealed to the opponent, implying that data protection is completely dependent on the key. If the opponent learns the key, the entire system is rendered inoperable until a new key is distributed

(Ogunlere, 2019). As illustrated in Figure 2.1, one key is utilized for each cryptography and cryptography in undisclosed Key Cryptography.

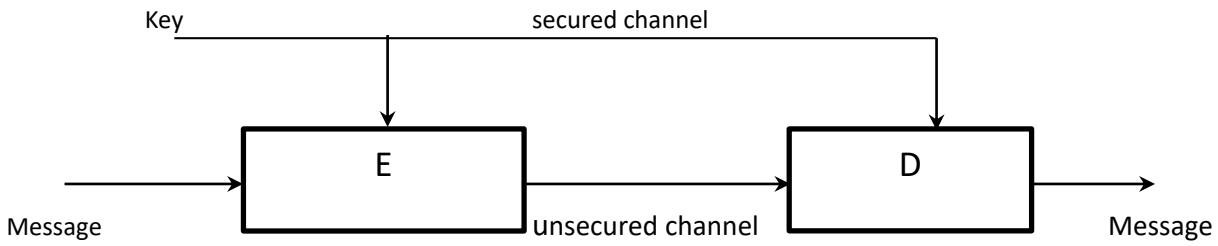


Figure 2.2 Secret Key Cryptography

IBM DES, a secret-key encryption method works on existing protocols. The National Institute of Standards and Technology Framework (NIST) began work on establishing a new safe cryptosystem for US government applications in 2014. (McLean, 2018). AES was founded because of DES and uses 128, 192, or 256 bits. When studying symmetric ciphers, the phrase block cipher is frequently used:

Block Ciphers

On the application of a cipher key k, a cipher block changes n-bit plaintext blocks to n-bit ciphertext blocks. The key is generated at random using various mathematical functions as shown in Figure 2.3

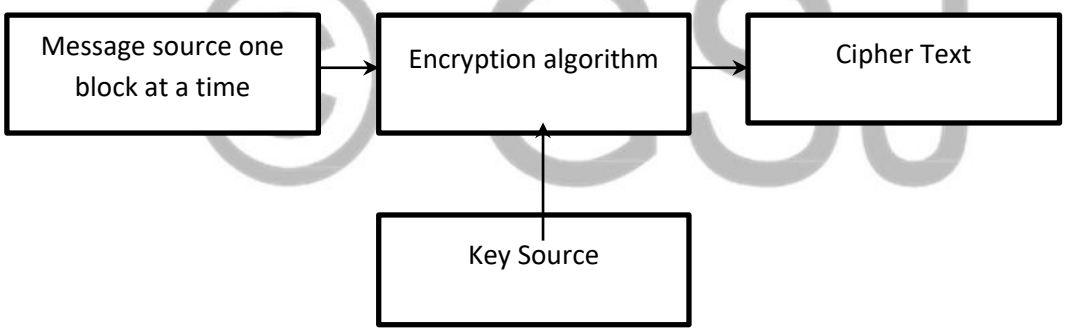


Figure 2.3 Block cipher

2.3 Encryption

Encryption techniques convert a plaintext message (or keep data) into ciphertext in such a way that the ciphertext exposes little or no information about the original plaintext (Kirst, 2015). Coding schemes are made up of three parts: a key generation rule, an associate coding rule, and a coding rule. The secret writing rule accepts plaintext and secret writing keys and returns the needed text in cipher (Metcalf, 2016). Today, coding protects people's and organizations' communications from naive and complicated criminals as well as undemocratic nations. It ensures the security of electronic commerce transactions over the internet, for example, by enabling the transmission of MasterCard numbers. It safeguards data stored on cell phones, computers, and other devices. Encrypted communication capabilities are built into key computer platforms in a variety of electronic messaging apps used by many people (Salama, 2017).

2.4 Encryption Applications

Cryptography is used in computer software, apps, and hardware to achieve goals that are important to the user. A single portable computer or smartphone, for example, nowadays often deploys coding in a variety of ways, including inside the hardware, the microcode that connects the hardware and the software package, and a significant amount of the software system that runs on the

device (McNally, 2018). The generality of encoding is relevant to public arguments over extraordinary access since only specific applications of encryption in a highly portable computer or smartphone alter the encoding of users' information of possible importance to law enforcement or intelligence services. As a result, the demand for extraordinary access would be obliged to be tailored to specific applications of cryptography where the specifics differ depending on the device (Shraddha, 2015). This section gives some highly simplified instances of a number of these applications, as well as how they rely on secret writing; the major focus is on revealing the function of encryption rather than complete implementation details.

a) Safeguarding Stored Files

Applications that protect one or more files usually utilize parallel cryptography to protect the file content (Murray, 2017). The key for the parallel cryptography system may also be entered into the program by the user, derived from user-supplied parole, entered from a hardware token, protected by an uneven cryptography system during which the parallel cryptography secret is encrypted beneath a public key and decrypted once the corresponding non-public secret is supplied, or some combination of those. For example, when a user registers into the Encrypting File system that is incorporated into Microsoft Windows, the operating system decrypts the user's private key (Singh, 2012).

Another application of encryption is to "delete" data. When information is encrypted and the secret is destroyed, the information is rendered unavailable, as if it had been deleted. Removing the secret is more important than deleting the information since losing the key renders all copies of the information unavailable (even backups) and eliminates the need to wipe storage media (Raina, 2016).

b) Encryption of the whole disk

Many contemporary operating systems enable complete disk encryption, which prevents the exposure of both user data and system applications. The files themselves, like the file secret writing situation printed on top of them, are safeguarded using secret writing (Bombale, 2013). Additional safeguards that combine. The whole disk Cryptography systems have advanced by a factor of two. The underlying hardware or microcode should have a method that validates a digital signature on the major microcode and software system parts that will be run once the system is booted, ensuring that they have not been maliciously altered. Once this validation is complete, and the user has authenticated the system with a passcode, token, or both, the hardware grants access to a secret (asymmetric) key, which the software system then uses to decode a keep symmetrical key, which is then used to decode the disk's contents (Vinayak, 2016).

d) Device Security

Mobile devices, and therefore the information they contain, are frequently safeguarded by lockup mechanisms that ensure, by default, that phone knowledge is encrypted whenever the screen is latched, and only the user may unlock the phone and its contents (Parker, 2015). This combination of cryptographic passcode security and full disk encryption was introduced as the default setting for phones in Apple's iOS and Android's Marshmallow systems, however, not all Android phone makers implement this encryption (Ndible, 2016).

The unlocking key might be a combination of the user's password and the phone's hardware key. When an erroneous passcode is entered, the phone pauses the next attempt. After a certain number of erroneous attempts, the key is destroyed, rendering the data unavailable. Users can configure their phones to use a biometric, such as a fingerprint or face, rather than a passcode; after a certain number of failed recognition attempts or a limited length of time, the phone reverts to the password unlock method (Mansoor, 2013).

d) Virtual Private Networks (VPNs)

A virtual private network (VPN) is a method of establishing an encrypted connection between an overseas user and a website. VPNs provide a simple way for companies to operate across different locations by allowing distant users to easily connect to the organization's networks. As a result, traveling employees may securely access their business network from a hotel room anywhere in the globe. VPNs function by employing symmetric cryptography to create information packets to be sent between central and distant sites and then embedding the encrypted packets in "outer" packets that are routed over the internet (Khan, and Khalid, 2013). The encrypted packets contain routing and other information that allows them to reach their destination inside the organization's network once decoded.

e) Protected Web Browsing

When a user accesses an e-commerce website or a Web-based email server like Gmail or Hotmail, he or she does it over an encrypted connection. TLS is a protocol that allows for an encrypted connection. It employs authentication methods that allow asymmetric cryptography and signed certificates to ensure that the server is the one whose name the user has typed into the browser. It then employs open-key encryption to generate a symmetric key for the browsing time, which is subsequently used to encrypt the

session communication. TLS or one of its predecessors is supported by almost all Web browsers and servers, and many web servers have the public-key certificates required to allow encrypted connections (Veerpal, 2015).

f) Encrypted Messaging

Secure electronic communication apps employ end-to-end secret writing techniques to prevent third parties from accessing the plaintext of communications due to the messaging service provider. The Signal protocol, developed by Open Whisper Systems, is utilized in several widely used electronic communication services, including Signal, WhatsApp, hidden chats in Facebook Traveler, Google Allo's "incognito mode," and Skype. When a user registers for an electronic communication service, the app transmits a public identification key, a public session set-up key, and a batch of public one-time session set-up keys to the electronic communication service's server while keeping the matching set of personal keys (Pipkin, 2013). To connect with other users, the starting app creates an encrypted session. To do this, the initiator's app asks a free-key server for a collection of public keys for the receiver. Both the creator and the receiver utilize each other's public keys to generate the session's master secret key. Then, using symmetric encryption, each communication is encrypted with a unique message key derived based on the master secret key (Shujaat, 2015).

g) Confidentiality Protection in Cloud or Third-Party Computing

Cloud computing and storage devices are altering how businesses utilize and manage their data, particularly their customers' data. E-mail services, such as Google's Gmail, and file storage and sharing services, such as Dropbox, are examples of consumer services that keep data in the cloud. Cloud services are often used to backup and recover data from cell phones and computers. Encoding is typically used to protect the secrecy of information. Depending on how the service is designed and the service provider's business model, the supplier may or may not have access to the keys necessary to rewrite the information (Rajinder, 2016).

2.5 Message Queuing

Message Queuing (MSMQ) allows users to link across webs and systems notwithstanding the present state of human action applications and systems. Applications transfer and accept messages over and over with message queues that MSMQ maintains. The message queues still operate even once the shopper or server application isn't running. Message queuing provides:

2.5.1 Asynchronous Messaging:

With MSMQ asynchronous messaging, applications from the client-side network with servers, return needed files immediately, even if the target computer or server program is not responding (Kumar, 2017).

2.5.2 Guaranteed Message Delivery:

When an application sends a message through MSMQ, the message will reach its destination even if the destination application is not running at the same time or the networks and systems are offline (Amritsar, 2015).

2.5.3 Routing and Dynamic Configuration:

MSMQ provides flexible routing over heterogeneous networks. The configuration of such networks can be changed dynamically without any major changes to the systems and networks themselves (Kumar, 2019).

2.5.4 Connectionless Messaging:

Applications using MSMQ do not need to set up direct sessions with target applications (Amit, 2020).

2.5.5 Security:

MSMQ provides secure communication based on Windows security and the Cryptographic API (CryptoAPI) for encryption and digital signatures (Zaiton, 2019).

2.5.6 Prioritized Messaging:

MSMQ transfers messages across networks based on priority, allowing faster communication for critical applications (Zaiton, 2019).

2.6 Publish/Subscribe Mechanism

Messages can be sent asynchronously to different sections of a system using the Publish-Subscribe paradigm (Shashi, 2019). A message topic, like a message queue, provides a lightweight method for broadcasting asynchronous event notifications as well as endpoints that allow software system elements to connect to the subject to send and receive such messages. A part is conceived of as a publisher just pushing a message to the subject to disseminate a message. Unlike message queues, which batch messages until they are retrieved, message topics transmit messages without or with little waiting and send them to all subscribers instantaneously (Mohiy, and Hatem, 2018). If no subscriber has a message filtering policy in place, any components that purchase the topic can get every message that is transmitted.

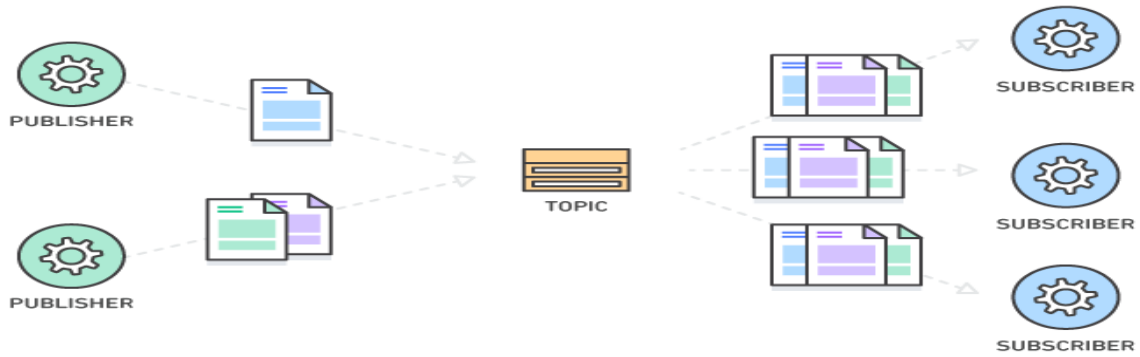


Fig 2.4 Publish/Subscribe Mechanism (Amazon, 2019)

The subscribers to the message topic usually perform different functions and may do one thing differently with the message in parallel. The publisher does not have to be compelled to recognize the data that it's broadcasting, and therefore the subscribers do not have to be compelled to recognize whom the message comes from. This style of messaging is a bit different than message queues, where the component that sends the message often knows the destination it is sending to (Vikas, 2019).

2.7 Design Technique

The technology comes in several forms, with key size and strength typically being the largest variations in one selection from consecutive.

Below is a unit of the techniques.

1. Triple DES: The triple encryption commonplace (DES) algorithmic rule was created to replace the initial encryption commonplace (DES) algorithmic rule, which hackers were able to defeat quite easily. Triple DES was previously the industry's recommended standard and, as a result, the most widely employed cruciform algorithmic rule. Triple DES employs three single keys, each of which is fifty-six bits long. Although the total key length adds up to 168 bits, experts claim that 112-bit key strength is a lot of love. Despite being phased out over time, Triple DES remains a reliable hardware encoding solution for money services and a variety of businesses (Hamzah Ahmad & Ruslan, 2020).

2. RSA: RSA is a public-key encoding algorithmic method. Because it uses a combination of keys, RSA is taken into consideration associate in nursing's uneven algorithmic rule, unlike Triple DES. You have a public key, which is what we usually use to encrypt our messages, and a non-public key to decode them. The consequence of RSA encoding could be a massive batch of data that requires a long time and a lot of processing resources to interrupt.

3. Blowfish: this is another algorithmic rule. Blowfish is renowned for its incredible speed and general effectiveness, as well as several claims that it has never been vanquished. Meanwhile, merchants have taken full advantage of the property right's free availability. Blowfish can be found in a variety of package types and is available as an encoding technique.

4. Twofish: Blowfish and its sequel Twofish were created by laptop security expert Bruce Schneier. The keys used in this algorithmic method might be up to 256 bits long, with only one secret required using the cruciform technique. Twofish is regarded to be one of the fastest of its kind and is suitable for application in a variety of hardware and software environments. Twofish, like Blowfish, is freely available to everyone who needs it by the World Health Organization. Encoding tools like Photo Encrypt, GPG, and TrueCrypt, the popular ASCII text file package, are used for it.

5. AES: Is the Advanced Encoding Standard (AES) a reliable algorithmic rule used by the United States Government and other organizations? AES encodes activities, despite being extremely cost-effective in 128-bit mode. Except for brute force, AES is regarded to be greaseproof to any attacks that attempt to decrypt messages using all possible combinations within the 128, 192, or 256-bit encryption. Nonetheless, security experts predict that AES will eventually be acclaimed as the de facto standard for encrypting data in the non-public sector.

2.8 Theoretical Framework

A theory can be defined as an assumption or a system of notions intended to clarify one specific topic, specifically one that is backed by numerous applicable principles. A theory is a large, interconnected collection of propositions. A theory can be correct or incorrect depending on the relevance and quality of knowledge at the time the theory is created, but a theory is never any kind of absolute truth (Roger, 2018). Think differently. According to this theoretical framework, a structure can serve as the foundation for a theory.

Theory of Technology

The application of computer security theories to create and evolve solutions that enable authentication, verification, non-repudiation, and validation is central to technology's response to security concerns. These theories and models rely on cryptography, steganography, network protocols, and software engineering processes/models to create systems that provide some level of protection for users and the information infrastructure. Insecurity thrives on the internet these days because the web failed to incorporate a mechanism that allows a host to actively refuse messages into its protocols from the start (Crocker, 2007).

This implies that a benign host that requires certain communications should scan all messages directed to it. In essence, a decommissioned or hostile server can broadcast any undesirable communications. This disadvantage is amplified by the internet's ever-present presence, and it remains the Achilles heel of the challenge of web security today. Although all the theories described above are related to law-breaking, we are inclined to apply routine activity theory to the current investigation because the hypothesis caught the philosophical assumptions on which this study is built (Schmalleger, 2012).

2.9 Review and Gaps in Past Studies

The Internet of Things (IoT) is rapidly expanding and offers several economic, sociological, and sociocultural potentials and benefits. However, the Internet of Things brings additional security, privacy, and safety risks (SPS). Existing work on mitigating these SPS concerns frequently fails to address the fundamental issues underlying the mitigation strategies proposed, as well as to establish relationships between completely distinct mitigation approaches (Harbers, and Bargh, 2018). Although both security and IoT have been around for a long time, none of the previous surveys provided a thorough examination of security risks associated with the Internet of Things. Several polls on IoT, specifically IoT security and privacy, have recently been released. All of these studies agreed on one thing: the limited environment and the rapid proliferation of IoT technologies (Varshney, 2018).

Previous research on IoT has not provided entirely comprehensive answers to security problems. All the surveys conducted have undoubtedly emphasized one similar element, namely the restricted environment and rapid expansion of IoT technology (Ritu, Sanjay, 2014). Despite these efforts, no substantial advances in security and privacy are apparent within the IoT sector, particularly inside cloud IoT systems, and there are numerous outstanding problems to overcome (Narender, and Anita, 2014). Despite these efforts, no substantial advances in security and privacy are apparent within the IoT sector, particularly inside cloud IoT systems, and there are numerous outstanding problems to overcome (Narender, and Anita, 2014).

The use of information systems has long been associated with concerns about user security and privacy (IS). The confidentiality, integrity, and availability of an asset are all protected from unauthorized disclosure, alteration, destruction, or interruption (Sattarova et al., 2000). Businesses have saved money on security in the long term by investing in high-end situations. The author discovered that "the more vulnerable the data is, the more money will be spent on information security." The higher the cost of vulnerability prevention, the riskier the project. According to the Ponemon (2015) report, the average cost of a data breach to a company increased from $376,000,000 in 2014 to $534,645,500 in 2015.

Version (2016) discovered that there were over 100,000 records in 2016, with 3,141 confirmed breaches. Hacker groups such as Anonymous have caused major firms to lose millions of dollars because of their operations. The actual cost was 126.875 billion dollars (Sandra, 2012). Cybercrime is the single most serious threat to national security, outranking all other forms of organized crime and general fraud combined (Armin, and Thompson, 2015). According to surveys conducted in recent years, Bugs and issues have been accumulating at an alarming rate (Schat, and Angelis, 2016). The possibility or danger that a device is exposed to harm that would result, and the time and resources required to accomplish a degree of protection are all factors in determining a device's security (Mulani, and Pingle, 2016). Organizations should focus on and raise awareness of information security concerns.

Fernandez et al. (2017) have identified many difficulties that can arise while utilizing existing security methods. Their research is based on a four-tiered IoT architecture that includes hardware, system software, network, and application layers. They also underline that addressing many of these difficulties will need a cross-layer co-design approach. Sweta K. Parmar, the author, did not go into detail on the challenges, and authentication mechanisms were lacking for the desired outcome. In their IoT contextual approach, they have highlighted the existence of people and intelligent things. Due to the variety of IoT systems, Sicari et al. (2012) identified issues in implementing existing security measures. Authentication, secrecy, and access control are also mentioned as critical security requirements. Vogel et al. (2010) used open architecture to satisfy the requirements of IoT systems. Flexibility, customizability, and extensibility are fundamental qualities of open architecture, allowing the system to change over time. Their approach, however, is devoid of

security and privacy. Furthermore, they have not taken a more comprehensive approach to essential IoT system features like interoperability, heterogeneity, autonomy, and mobility.

According to past research, significant security and privacy problems exist in restricted, heterogeneous, and fast-increasing IoT domains. As a result of these issues, numerous security criteria, including authentication, authorization, confidentiality, and so on, are imposed. However, none of these studies provide a comprehensive review of the various types of security and privacy-related concerns that exist, as well as how to handle them early in the software development lifecycle.

To address security and privacy within the IoT domain, several academic research were carried out and Security is an industry initiative to assist in gains that can be seen in the IoT business, particularly in open IoT systems, and various hurdles The revealed work focused on security. In addition, the article involves looking at progress in cryptography methodology to gain how security is achieved on internet-abled devices. Patel and Crowcroft's efforts were focused on mobile device security resolutions (Sonepat, 2009).

Czerwinski et al. (2013) use uneven cryptography for authentication as well. Stajano and Anderson (2014) highlight the issues that arise when security devices are bootstrapped. Their solution requires the new gadget to make physical contact with a master device to imprint certain hidden information. Chou and Hass propose using asymmetric cryptography to secure ad-hoc networks. Carman, Kruus, and Matt (2014) investigate a wide range of approaches to key agreement and key distribution in detector networks. They investigate the overhead of these protocols on various hardware platforms. Some academics are looking into the possibility of providing cryptology. The steps proceed from the hard part to recursive cryptography work.

Many systems combine various secret protection tools and techniques. Secure AVR controllers, Fortezza government standard, and hence the Dallas iButton are examples of such systems. These systems support primitives for public-key encoding, with conventional operation instructions, and decide to zero out their memory if a state change is detected. These devices, however, were created for a variety of applications and are not intended to be low-power gadgets. The majority of the research on cryptological algorithmic rules for low-end devices relies on centrosymmetrics. Because of their low overhead, centrosymmetric coding techniques appear to be intrinsically compatible with low-end devices. Low-end microprocessors, on the other hand, are just. As a result, implementing many centrosymmetric ciphers on our target architecture is prohibitively expensive.

The attack vector is expanding in tandem with the number of connected devices. Traditional strategies for protecting devices from public networks are still available on the market, but they need to be reconsidered when applied to IoT systems and devices. These security concerns include Trust Management, Authorization, Authentication, Identification, Access Management, Network Security, Standardization, and Security Capability, among other things. Given the rapid evolution of IoT technology, the amount of private information being shared between connected devices in a matter of seconds, and an expanding spectrum of attack surfaces and attack vectors, the significance of this thesis is highlighted. The primary goal of this investigation is to secure IoT devices by ciphering and rewriting knowledge with the Advanced Encryption Standard (AES).

3.0 METHODOLOGY

In conducting this research to achieve the specified objectives of creating a security system for IoT devices, a straightforward methodology will be employed. The approach involves collecting security challenges faced by Internet of Things (IoT) devices, filtering these challenges, and subsequently applying an encryption algorithm to the filtered challenges to establish a secure communication method for IoT devices. This chapter will comprehensively outline the research development tools and framework selected, justifying the chosen tools to effectively realize the stated aims and objectives of the research.

3.1 Problem Definition

The prevalent practice in numerous establishments and regulatory bodies is the endorsement or requirement of encrypting sensitive information to prevent unauthorized access by third parties or malicious actors. In scenarios where a sensitive document is secured with an encryption password, the challenge arises when the document needs to be opened and decrypted by the recipient using the same password used for encryption. The critical issue lies in securely transmitting this password over the internet to the recipient without it being vulnerable to hacking threats. Traditional methods, such as email, pose risks and unreliability due to security concerns, potentially exposing the password to unauthorized access during transmission. This identified problem underscores the necessity for a comprehensive study to address the secure transmission of encryption passwords in a networked environment.

3.2 Design and Algorithm

The research project will implement an asymmetric encryption design to address the challenge of securely transmitting password-protected information over the internet. Symmetric encryption involves the use of a key, a secret code or phrase chosen by the user,

to transform the content of a message by combining it with other text in a specific manner. The study will generate both public and private keys in the implementation of asymmetric encryption.

The study was made of cryptography -encryption algorithm.

The art of safe communication is the science of cryptography. The goal is to communicate the information securely, without a third party getting the message. This is a significant concern because it opens options for improving the security of devices. The entire linked gadget serves as an endpoint that is vulnerable to hackers.

Protecting what you have even if you don't have millions to lose is critically important. It is widely believed that every device user should know how to use encryption.

Secret key (symmetric): Both encryption and decryption are done using the same key.

Asymmetric (public key): It uses two separate keys for encryption and decryption, one of which is a public key.

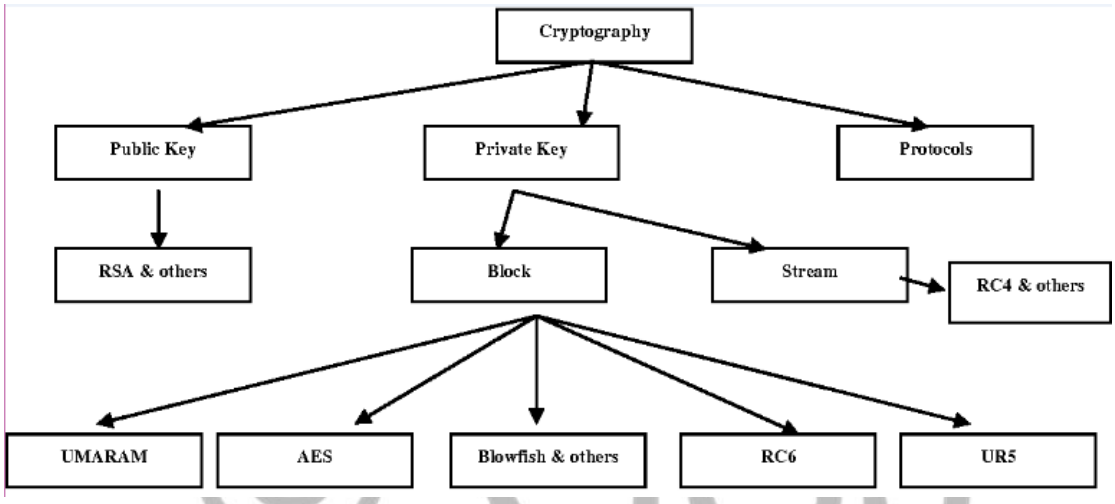


Figure 3.1 shows cryptography processes (Shankar, & Jenifer, 2017).

The encryption algorithm is a technique used to convert data into ciphertext. Encryption is the action of changing plaintext into something called ciphertext and this is by a means called cipher or encryption algorithm. The cipher uses the key to encrypt data. The idea behind it is that the encryption should not depend only on the cipher algorithm, and it should be secure. Further to security, the introduction of encryption is often motivated by the need to meet submission regulations.

Advanced encryption standard (AES) is a very fast and secure system of encryption that stops snooping eyes away from data. Advanced encryption standard is used in messaging apps like programs like Vera-crypt, WhatsApp and Signal, and WinZip, in a range of hardware and variability of other technologies.

3.3 Steps in the Encryption and Decryption Model

The Steps employed are:

1 First an exchanging of public keys between entities (sender and receiver).

2 sensitive documents are encrypted and sent with the sender's public key.

3 receivers decrypt the document using its private key to unlock the document.

4 The strength and security of asymmetric encryption rely on the sender and receiver to keep their private key well-protected.

Encryption Algorithm

The whole setup is to keep intruders out of sensitive data that could affect the integrity of the message which may harm the network and devices connected. The advanced encryption algorithm (AES) works on the block cipher technique. The size of the plain text and ciphertext must be the same. Advanced encryption algorithm consists of multiple rounds of processing different key bits like 10 rounds for processing 128-bit keys, 12 rounds for processing 192-bit keys, and 14 rounds for processing 256-bit keys. The encryption follows each round of the following four steps:

01. Sub Bytes
02. Shift Rows
03. Mix Columns
04. Add Round Key

This algorithm is designed with 128 bits of block size and key size, respectively, AES generates ciphertext of 128 bits for 128 bits of plaintext. From the early round, plaintext progresses through ten rounds. All-round contains procedures like shift rows, byte substitution, shift rows, add round key, and mix columns, and add round key.

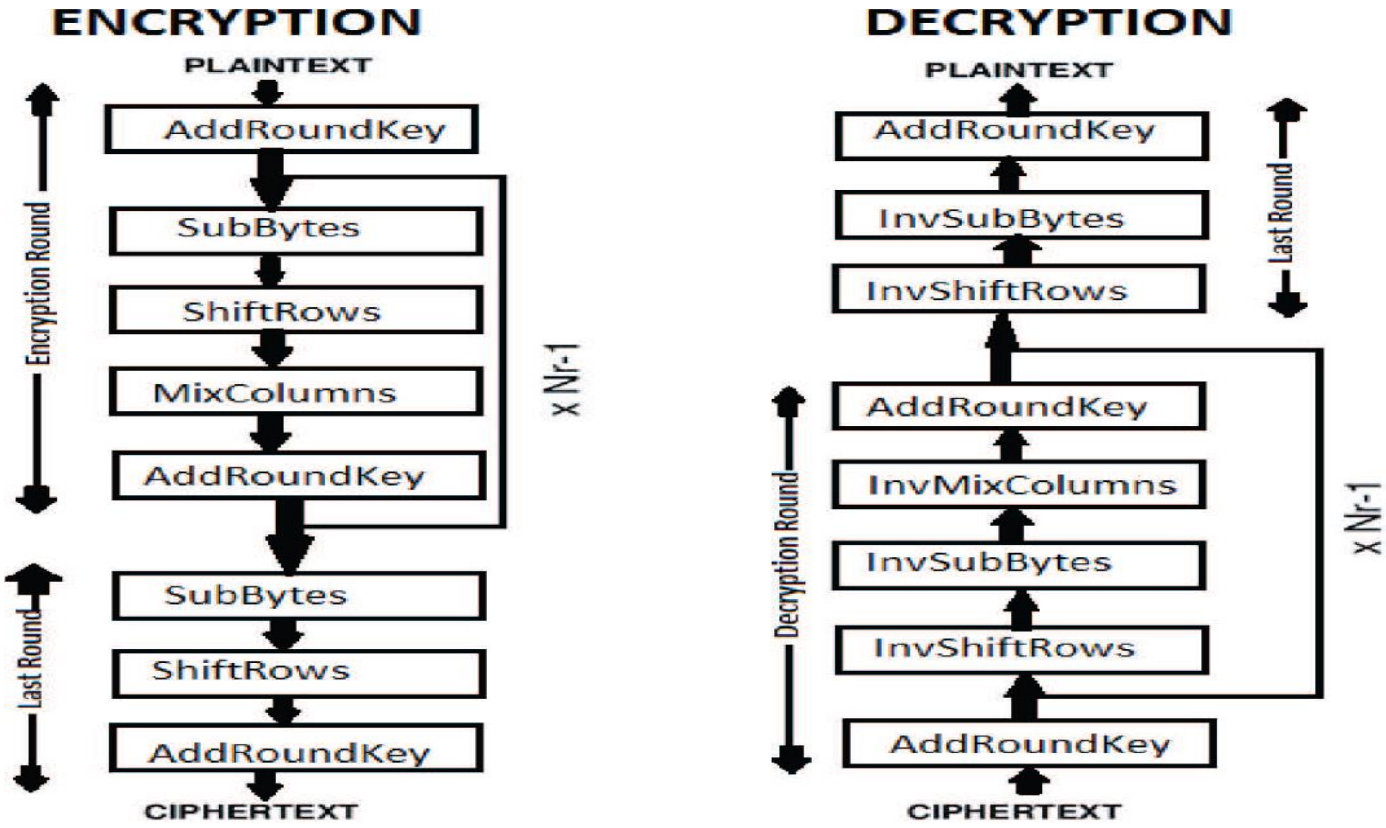


Figure 3. 2 Overall structure of AES algorithm Source from Beg (2018)

ALPHABET	DECIMAL REPRESENTATION	HEXADECIMAL REPRESENTATION
A	00	00
B	01	01
C	02	02
D	03	03
E	04	04
F	05	05
G	06	06
H	07	07
I	08	08
J	09	09
K	10	0A
L	11	0B
M	12	0C
N	13	0D
O	14	0E
P	15	0F
Q	16	10
R	17	11

33

S	18	12
T	19	13
U	20	14
V	21	15
W	22	16
X	23	17
Y	24	18
Z	25	19

Figure 3.3 shows the process of the decryption of the algorithm,

3.4 Source of Data on Transition

Data in the form of messages will be moved in real-time from communicating device A to listening device B to interpret and communicate with. To achieve the objectives of this project, we introduce encryption.

3.5 Repository Assist of Message on Transit

Microsoft Message Queue will be used as a repository should a listening device not be available to access the message in transit in real-time should there be no internet connection at the time of sending the message.

Message Queuing (MSMQ) technology permits applications running at completely different times to speak across heterogeneous networks and systems that will be briefly offline. The applications will send messages to the queues and might conjointly browse messages from queues. Below is an associated illustration showing how a queue will hold messages that are generated by many sending applications and read by numerous receiving applications.

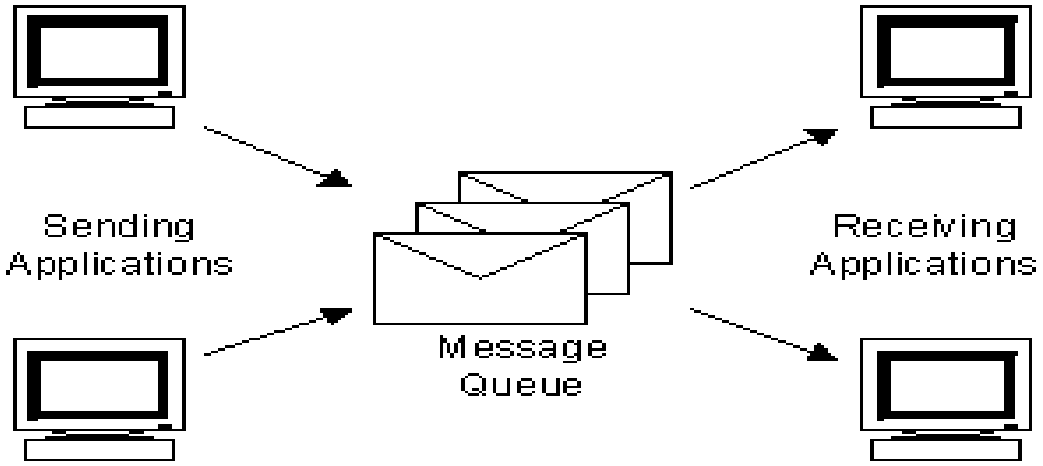


Figure 3.2 Message queue (Anush, 2017)

Message Queuing provides bonded message delivery, economical routing, security, and priority-based electronic messaging.

It will be wont to implement solutions to each asynchronous and synchronous situation requiring high performance. The subsequent list shows many places where Message Queuing will be used.

1. Mission-critical money services: as an example, electronic commerce.

2. Embedded and hand-held applications: as an example, underlying communications to associate degrees from embedded devices that route baggage through airports by suggesting an automatic baggage system.

3. Outside sales: as an example, sales automation applications for traveling sales representatives.

4. Workflow: Message queuing makes it straightforward to form progress that updates every system. A typical style pattern is to implement an associate degree agent to act with every system. Exploitation workflow-agent design conjointly minimizes the impact of changes in one system on the opposite systems. With Message Queuing, the loose coupling between systems makes upgrading individual systems easier.

All key lengths will be to shield the confidential and secret levels. Top undisclosed info needs either 192 or 256-bit key sizes. There are ten rounds for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for 256-bit keys. A round consists of many process steps that embrace substitution, transposition, and a mixture of the input plaintext to rework it into the ultimate output of ciphertext.

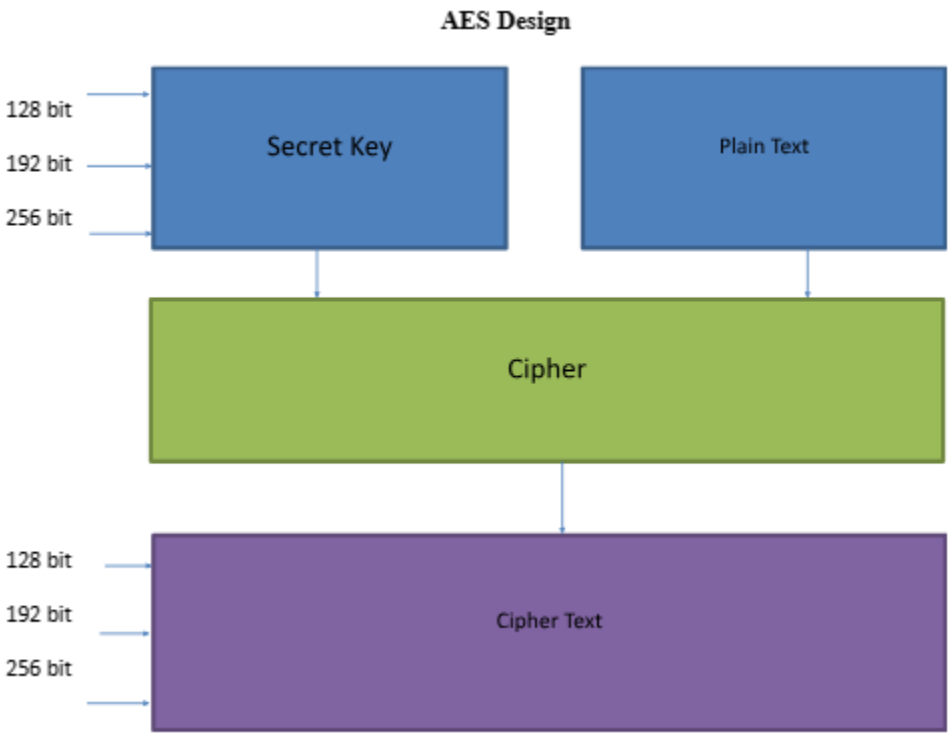


Figure 3.3, AES design operation (Researcher, 2021)

3.6 Encryption Operation

The diagram below displays the connection between the Secret key, Cipher, Plaintext, and Cipher Text, all of which are elements of the AES encryption method. The initial stage in the encryption process is to place the data into an array. Then, the encryption transformations are performed several times throughout many rounds of encryption. In the first step of the AES encryption cipher, the substitution of data using a substitution table is carried out; the second step is the shifting of data rows, and the third step is the mixing of columns. Every column utilizes a different piece of the cryptographic key for the last change. Longer keys would like additional rounds to finish.

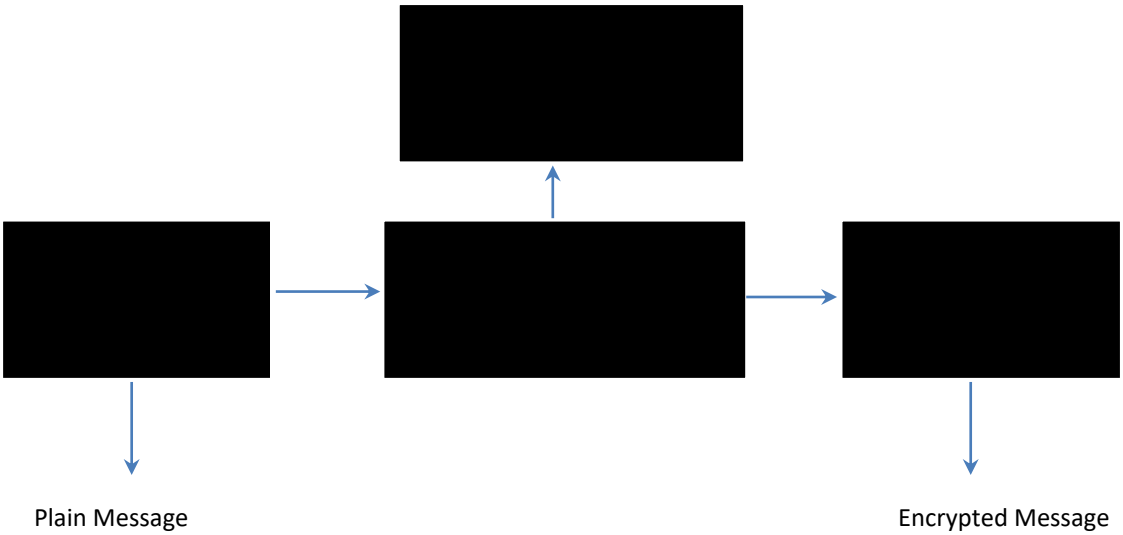


Figure 3.4: Encryption operation (Researcher, 2021)

3.7 Development Tools

Details and justification of the event tools are mentioned ranging from Microsoft Visual Studio IDE.

Microsoft Visual Studio and Dot Net Framework

Microsoft Visual Studio is an IDE that supports web development. Due to years of developing web apps, such as websites, web apps, internet services, and mobile apps, users were more likely to make them themselves. They are all used by Visual Studio when creating apps. Ultimately, it will wind up in every code that is native and managed. IntelliSense, a code completion component, is included in Visual Studio as a code refactoring feature. Every source-level program and a machine-level program are included in the integrated program. Reinventing the way things are done includes making use of a code profiler, a form designer, and an information schema designer. Visual Studio exists in versions and the current version is Visual Studio 2019 (Brett Lopez, 2019).

The Microsoft Dot Net framework additionally termed .Net framework, a code development platform developed by Microsoft will be used. The framework provides support for multiple programming languages like F#, C#, Visual Basic, and Python.

Programming Language

The study will make use of the C# programming language. The programming language simplifies several of the complexities of alternative higher-level languages and provides powerful options like null-able worth varieties, delegates, enumerations, lambda expressions, and direct operation that isn't found. The languages area unit was chosen as a result of its quick operations, object-oriented in nature, cross-platform, ability, easy readying, automatic pickup, higher integration, and rejection of memory leak, most helpful and powerful, high motivation towards work with abundant support of the programming language from Microsoft.

3.8 Limitations of the Study

Using C-sharp language on Visual Studio for security alone is proscribed. Encrypting and decoding information across IoT devices could suffer from quality labor problems. so, the findings, and observations, emanating from this study ought to be considered and understood within the lightweight of the limitations inherent during this work and therefore the application to sensible functions valid up to now because the limitations would allow.

Below the table is the inverse S-box. It will be used during the decryption process.

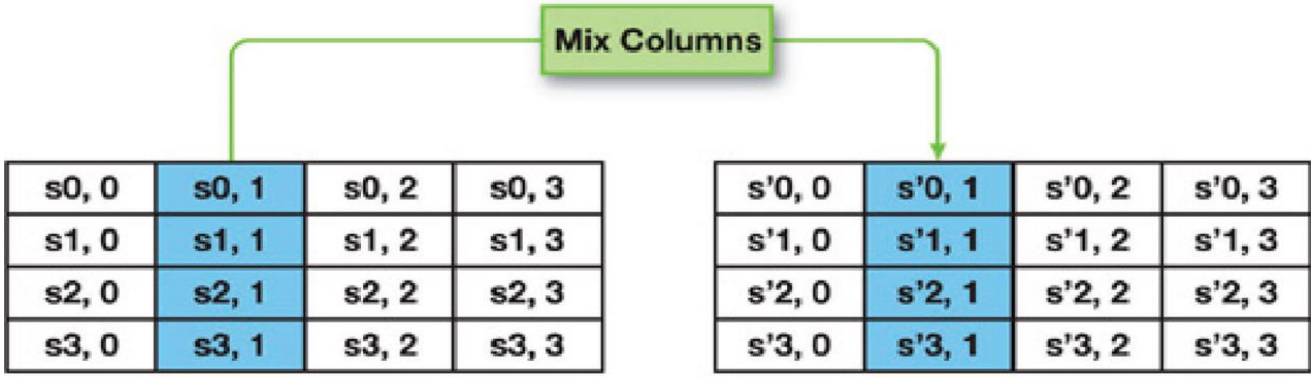
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	82	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	89	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	84	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	87	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	38	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Fig 3.3a: S-box AES Algorithm (Ramirez-Torres MT, 2018)

01. Sub Bytes/Substitute Bytes:

The 16 input bytes are substituted by using a fixed lookup table known as an S-box. This s-box consists of all possible combinations of 8-bit sequences. The first four bytes of a 128-bit input block occupy the first column in the 4×4 matrix of bytes. The next four bytes occupy the second column and so on.

The mixed columns operate on each column individually. This task takes four bytes of the column as input and outputs, which is a completely new four bytes that substitute the unique four bytes. Each byte of a column is plotted into a new value which is a function of all four bytes in that column.



$$\begin{pmatrix} s'0,1 \\ s'1,1 \\ s'2,1 \\ s'3,1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} s0,1 \\ s1,1 \\ s2,1 \\ s3,1 \end{pmatrix}$$

Transform Matrix of Mix Columns

Fig 4.6: Mix column of AES Encryption (Researcher, 2021)

The mix columns theory is calculated using the formula above. Where, S0, S1, S2, and S3, are the results after the transformations. S'0, 1 – S'3, 1 can be obtained from the matrix after the data undergoes a substitution process in the S-Boxes.

3.9 Performance Test

The study will incorporate Performance Testing, specifically Component Testing, to evaluate individual components or units of the software. This form of testing involves isolating a section of code and verifying its accuracy. The focus of the performance test will be on the encryption and decryption phase of the code. Microsoft C# and .NET infrastructure will be employed for testing the code.

Summary

The primary issue identified is the transmission of plain text over the internet, posing a risk to sensitive documents secured with an encryption password program. The challenge arises when the receiver needs to decrypt the document using the same password and transmitting the password over the internet exposes it to potential hacking and snooping threats.

To mitigate this risk, the study proposes the implementation of asymmetric encryption, involving the generation of two keys—one private and one public. This approach ensures secure encryption and decryption processes without transmitting sensitive passwords. The choice of asymmetric encryption is influenced by the consideration of low computer resources and the use of conventional web frameworks platforms, such as VSC (Visual Studio Code), Microsoft Dot Net framework, and C# Programming Language, which simplifies complexities in security designs and software functions. The study seeks to investigate and implement this solution to contribute to the advancement of IoT security.

The anticipated outcome of this project revolves around the implementation of encryption algorithms for securing IoT devices. Employing the C# programming language within Microsoft's integrated development environment, the research aims to ensure data availability, confidentiality, and protection against intrusions. The utilization of asymmetric encryption design serves as a solution to the challenge of password protection during internet transmission. Secret keys, being any computer-acceptable number and words, are employed in Symmetric Encryption. The asymmetric system involves generating the necessary means to ensure the success of both encryption and decryption processes.

The expected finding is that plaintext will be encrypted as designed, rendering it indecipherable to third parties, except for the intended recipient. This will represent an improvement over previous academic research, such as that of Harbers and Bargh (2018),

Varshney (2018), and Fernandez et al. (2017), which was primarily limited to literature reviews without considering crucial IoT system properties like interoperability, heterogeneity, autonomy, and mobility comprehensively. The anticipated result reinforces the notion that IoT devices can be effectively protected.

Conclusion

The upcoming work involves the development of an encryption-decryption program model utilizing public and private keys for securing internet-based information. The encryption and decryption process, facilitated by a cipher object, aims to safeguard digital data privacy and address ethical concerns related to the connected system. Employing an asymmetric algorithm in symmetric key encryption ensures the protection of data through block cypher techniques for both encryption and decryption operations. Key lengths are strategically chosen to preserve confidentiality, and additional processing steps, involving transformation and mixing of the text, contribute to achieving the desired outcomes. The program will leverage Message Queuing (MSMQ) technology to enable applications to interact across diverse networks and systems with varying availability. By efficiently securing data transmitted over the internet and optimizing memory space utilization against recovery tools, the program aims to enhance overall information security.

Acknowledgment

The authors wish to thank the almighty God who is the keeper and preserver of life, who gives knowledge without limits.

References

1. Abdel, K. A. T. (2017). “Performance analysis of data encryption algorithms,” Retrieved from http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf.pdf
2. Abdul, E., Kader, A., & Mohie, H. (2008). “Performance evaluation of symmetric encryption algorithms,” IJCSNS International Journal of Computer Science and Network Security.
3. Abdul, M., Kader, D. S., Abdul, H. M., & Hadhoud, M. M. (2001). “Analysis of performance for symmetric cryptography.”
4. Abdullah A. (2017). "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Cryptography and Network Security,” Ryptography and Network Security, 16, 1-11.
5. Abd Zaid M. and Hassan S. (2019). “Modification Advanced Encryption Standard for Design Lightweight Algorithms,” Journal of Kufa for Mathematics and Computer, 6(1), 21-27.
6. Agrawal, M., & Pradeep, M. (2012). “A comparative survey on symmetric key encryption techniques,” Retrieved from http://www.enggjournals.com/ijcse/doc/IJCSE 12-04-05-pdf
7. Ajay, K., Singh, M. L., and Bansal, P. K. (2012). “Comparison of various encryption algorithms and techniques for secured data communication in the multi-node network”, IJETInternational Journal of Engineering and Technology.
8. Akash, M., Chandra, P., & Archana, T. (2016). “Performance evaluation of cryptographic algorithms: DES and AES,” IEEE Students ’Conference on Electrical, Electronics and Computer Science.
9. Alanazi, O., Zaidan, B. B., Zaidan, A. A., Jalan, A., Shabbir, M., & Al-Nabhani, Y. (2015). “New comparative study between DES, 3DES, and AES within nine factors,” Journal of Computing.
10. Alese, B. K., Philemon E. D., Falaki (2012). “Comparative Analysis of Public-Key Encryption Schemes.”
11. Ali Ahmad Milad, Hjh Zaiton Muda, Zul Azri Bin Muhamad Noh, and Mustafa Almahdi Algaet (2012). “Comparative Study of Performance in Crypto”graphy Algorithms.”
12. Ali Makhmali, Hajar Mat Jani (2013). “Comparative Study on Encryption Algorithms and Proposing, A Data Management Structure.”
13. Ankita Umale,, Ms. Priyanka Fulare (2014). “Comparative Study of Symmetric Encryption Techniques for Mobile Data Caching in WMN.”
14. Apoorva, Yogesh Kumar (2013). “Comparative Study of Different Symmetric Key Cryptography Algorithms.”
15. Chinmoy Ghosh and SatyendraNath Mandal (2014). “A Combined Method for Image Encryption.”
16. Choi I. and Kim J. (2016). "Area-Optimized Multi-Standard AES-CCM Security Engine for IEEE 802.15. 4/802.15,” Journal of Semiconductor Technology and Science, 16(3), 293-299.
17. Daniel Wichs (2012). Barriers in Cryptography with Weak, Correlated and Leaky Sources.
18. Er. Satish Kumar, Amritsar Mr. Amit Puri (2012). “Comparative analysis of the various cryptographic algorithms.”
19. Espressif Systems. (2020). "ESP-IDF Programming Guide,” https://docs.espressif.com/projects/esp-idf/en/latest/esp32/.
20. Feng Bao Pierangela Samarati Jianying Zhou (2012). “Applied Cryptography and Network Security,” Pranay Meshram, Pratibha Bhais
21. G. Ramesh and Dr. R. Umarani (2012). “Performance Analysis of Most Common Symmetrical Encryption Algorithms.”
22. Govinda Rao, D. Siva Prasad, and M. Eswara Rao (2013). “Universal Session-Based Symmetric Cryptographic Technique to Strength the Security.”
23. Hamzah H., Ahmad N., and Ruslan S. (2020). “The 128-Bit AES Design by Using FPGA,” Journal of Physics: Conference Series, 1529(2), 022059.

24. Hussein N. and Shujaa M. (2020). “DNA Computing Based Stream Cipher for Internet of Things Using MQTT Protocol,” International Journal of Electrical and Computer Engineering, 10(1), 1035.
25. Inamdar A. (2020). "ESP32-S2-Security Features,” The ESP Journal. https://medium.com/the-esp-journal/esp32-s2-security-improvements-5e5453f98590.
26. Jitendra Shetland and Harsh Gupta (2014). “Comparative Study of a New Variable-Length Key Block Cipher Technique with DES for Network Security.”
27. Johannes Blömer, Peter Günther, and Gennadij Liske (2012). “Improved Side-Channel Attacks on Pairing Based Cryptography.”
28. K.Brindha, Ritika Sharma, Sapanna Saini (2014). “Use of Symmetric Algorithm for Image Encryption.”
29. Khoa T., Nhu L., Son H., Trong N., Phuc C., Phuong N., Dung N., Nam N., Chau D., and Duc D. (2020). "Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study." Wireless Communications and Mobile Computing,” 2020, 1-18.
30. Kodali R. and Soratkal S. (2016). "MQTT Based Home Automation System Using ESP8266,” Proceedings of IEEE Region 10 Humanitarian Technology Conference, Agra, 1-5.
31. Kouicem D., Bouabdallah A., and Lakhlef H. (2018). "Internet of Things Security: A Top-Down Survey,” Computer Networks, 141, 199-221.
32. Mansoor Ebrahim, Shujaat Khan and Umer Bin Khalid (2013). “Symmetric Algorithm Survey Comparative Analysis.”
33. Ms.Pallavi H.Dixit, Dr.Uttam L. Bombale, and Mr. Vinayak B. (2013). “Comparative Implementation of Cryptographic Algorithms on ARM Platform.”
34. Nandhini P. and Vanitha V. (2017). “A Study of Lightweight Cryptographic Algorithms for IoT," International Journal of Innovations and Advancement in Computer Science, 6(1), 26-35.
35. Narender Tyagi and Anita Ganpati (2014). “Comparative Analysis of Symmetric Key Encryption Algorithms.”
36. Parida D., Behera A., Naik J., Pattanaik S., and Nanda R. (2021). “Real-time Environment Monitoring System Using ESP8266 and Thing Speak on Internet of Things Platform.”
37. Rajinder Kaur, Er. Kanwalpreet Singh (2013). “Comparative Analysis and Implementation of Image Encryption Algorithms.”
38. Ritu Tripathi and Sanjay Agrawal (2014). “Comparative Study of Symmetric and Asymmetric Cryptography Techniques.”
39. Sheetal Charbathia and Sandeep Sharma (2014). “A Comparative Study of Rivest Cipher Algorithms.”
40. Swati Paliwal, Ravindra Gupta (2013). “A Review of Some Popular Encryption Techniques.”
41. T.Gunasundari and Dr. K.Elangovan (2014). “A Comparative Survey on Symmetric Key Encryption Algorithms.”
42. Veerpal Kaur, Aman Singh (2013). “Review of Various Algorithms Used in Hybrid Cryptography.”
43. Vishwa Gupta, Gajendra Singh, and Ravindra Gupta (2014). “Advance cryptography algorithm for Improving data security.”