International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Design and Implement Technique for Security of IoT-5G System using RSA Algorithm

Pratik Shah *[1], Dr. Deepika Pathak[2]

Submitted: 04/11/2023 **Revised**: 21/12/2023 **Accepted**: 03/01/2024

Abstract: IoT stands for Internet of Things. The aim behind the development of IoT is to create a network of several objects and devices that are well connected with each other through wireless or wired Internet to exchange data with one another and to perform any action based on the received input. In today's era IoT is providing social as well as economic growth to country by developing several products and application. It provides applications and services in various areas like manufacturing, monitoring environment, food processing, transport, security, health care and surveillance. These applications and services are well connected with networking, cloud computing, decision making, data security, decision making and machine to machine communication. There are several characteristics and advantages of IoT but there are some disadvantages and threats also exist with this technology. IoT devices are not secured and can be easily hacked or malfunction because a cyber attacker can send a virus to the device and the device could be damaged or may perform certain wrong operations as a result huge loss may occurs. Well known threats related to IoT and Computer Networks are Denial of Service attack, Chosen Cipher text attacks, Distributed Denial of Service attack, Man in the Middle attack etc. While designing such solutions for IoT, one must consider that these devices have less storage capacity and lesser processing speed. Hence the design of the solution must be light and have extra strong cryptography. In this paper following tasks have been performed to achieve data security goals for IoT-5G. Boltzmann Machine is used to generate secured keys. Its performance is compared with other methods to generate keys, encryption and decryption time. Performance Enhancement of RSA algorithm have been done and further it's performance is compared with existing versions of RSA. During result analysis it is found that the above methodology works better than existing solutions.

Keywords: *Wireless, Communication, Migrate, Security, Automation, IoT-5G, Boltzmann Machine.*

1. Introduction

IoT stands for Internet of Things. The aim behind the development of IoT is to create a network of several objects and devices that are well connected with each other through wireless or wired Internet to exchange data with one another and to perform any action based on the received input [1]. In today's era IoT is providing social as well as economic growth to country by developing several products and application. It provides applications and services in various areas like manufacturing, monitoring environment, food processing, transport, security, health care and surveillance. These applications and services are well connected with networking, cloud computing, decision making, data security, decision making and machine to machine communication. There are several characteristics and advantages of IoT but there are some disadvantages and threats also exist with this technology [2]. IoT devices are not secured and can be easily hacked or malfunction because a cyber attacker can send a virus to the device and the device could be damaged or may perform certain wrong operations as a result huge loss may occurs. Well known threats related to IoT and Computer Networks are Denial of Service attack, Chosen Cipher text attacks, Distributed Denial of Service attack, Man in the Middle attack etc [3].

Security and privacy of IoT devices and computer network is a prime concern now a days and hence the challenge is to develop a secured and safter IoT solution so that Data Integrity, Authentication and Confidentiality could be achieved [4]. While designing such solutions for IoT, one must consider that these devices have less storage capacity and lesser processing speed. Hence the design of the solution must be light and have extra strong cryptography [5].

1,2Department of Computer Science and Engineering
1 Research Scholar, Dr. A. P. J. Abdul Kalam University, Indore
2 Research Supervisor, Dr. A. P. J. Abdul Kalam University, Indore
E-mail Id: 1pratikshah009@yahoo.com, 2deepikapathak23@gmail.com
** Corresponding Author: Pratik Shah*
Email: pratikshah009@yahoo.com

1.1 Internet of Things

IoT is used to establish a connection between several electronic devices with the help of various wireless technologies. In the past few years IoT has boosted the growth of technology and has been successfully captures the growth of the market [6]. IoT devices generally use sensors to collect the data from their surrounding environment and process the data for further action using Internet. To work in such an environment each IoT device or object must have capabilities to communicate, store and also a unique physical address [7]. Since IoT has created a self-centered world which is well organized, smart, always ready to learn from the past data and adaptive network, it has a numerous application in agriculture monitoring soil moisture & greenhouse effect, high-tech smart cities parking management & observation of patient health, water management leakage & water level detection, forest fire detection, air pollution etc. The main challenge is to provide a secured and confidential communication system, so that data could be always remains untouchable from hackers [8]. Since for any organization or any human being data is always a prime concern, no one wants to compromise on data security, integrity and privacy.

Fig 1: Applications of IoT

Demand of IoT enabled devices and products is increasing day by day, these devices work with very less human intervention i.e., automation is also increasing on a very rapid pace [9]. There are several companies that manufacture different products & devices, all these devices share data and does communication using Internet. IoT have mainly two components Internet and Things. Internet refers to network of networks, which provides a way to share resources and data among several objects [10]. Things refers to various devices that range from street light, home lights, toast makers, airplanes, dust bin, cars, bikes, air conditioner etc. These devices have several applications in shopping malls, education, agriculture, hospitals, smart city etc. Hence, we can summarize it in the following manner that IoT is a setup where several devices work in a smart manner by transferring data using Internet [11]. IoT aims to have lesser interaction between human to machine but more and smooth communication between machine to machine [12].

1.2 Domain Specific Applications

IoT is now capturing the market by providing world class intelligent machines and devices at reasonable price, as a result of this new business establishment is done for application developers, hardware manufacturers and Internet Service providers. According to [13] by the end of 2025, hardware manufacturing companies will generate a business of $5 trillion and Internet consumption will also be double than the current scenario. Electricity smart grid technology will have 10% of the total market share than the present one which is about 7%. Applications of IoT health care products will reach to 46% and manufacturing companies will have 35% IoT enabled machineries [14].

Beyond these predictions, the applications of IoT in health-care has a share of 41% and followed by manufacturing industry with 33%. Certainly, in upcoming years use of IoT enabled devices will gain more attention in Agriculture & Security [15]. IoT devices are also now part of 2% vehicle, with such huge figures, lets start discussion of few domains' specific applications in the coming section [16].

- Smart Cities
- Intelligent Home
- Smart Agriculture & Environment
- Intelligent Grid System
- Smart Manufacturing Sector
- Smart Health Care

1.3 Security issues in IoT

Internet of Things is basically a set of connected electronic devices using wired or wireless Internet. In the last decade IoT has gain more popularity because of its usability increased in several areas like education, transportation, manufacturing etc.

Journey of IoT is started in 1960 during those days embedded Internet invented, but the term IoT invented

in 1999 for promoting the concept of Radio frequency identification which was build up using sensors and finally in the year 2010 IoT has started gaining popularity [17]. In the same year Chinese government have given a five-year plan to develop IoT devices in their country and today in the world approximately 30 billion devices exist in the world because now a common man and every house it is part of our daily life in the form of smart electric meters, smart watch & smart cities. This rapid development and consuming environment generated a huge business, improved the business environment and in such manner now IoT is part of everyone life by providing automation [18]. Due to such rapid growth data security and privacy issues were compromised. People use these devices without any concern, no change in passwords for years, no software upgradation of the device leads to risk of the data produced by the device. Due to weaker security protocols and adaption of poor data policies, most of the data security experts consider IoT devices are easy to hack or malfunction. There exists several security mechanism and measure to protect IoT devices from hackers and cyber attacks but still data security guidelines and recommendations were not followed properly as a result of this end users are not able to protect their data against these attacks [19]. Cyber-attacks started in 2008 for IoT devices and different viruses were used to malfunction the device.

Manufacturing companies' area using IoT enabled devices from a long time to control the production and machineries using application software's to gain competitive advantage over the competitors, but due to massive adoption of these devices leakage of data became a concern for most of the business. As a result of this a data security professional is required which can measure the threats and can take proper action on time so that services should not be disturbed.

This is the era of computer science, every day some new technology born or upgradation to the existing one happens. In the field of telecommunication 5G network came in 2023. The superfast network 5G is expected to play an important role for IoT devices and applications. Research is going on to find out the privacy and security risk of data in this fast network [20]. It is important to find out the possible risks and to develop possible solution to the risk.

In this research, our target is to provide description of IoT devices, their applications, benefits, identification of possible risk and its solution [21]. Before coming to solution a through literature review will be done, to gain knowledge from existing data security algorithms and techniques. Thereafter a solution will be proposed, will be implemented and the results will be compared with the existing solutions to evaluate the performance of the solution. This work will provide a base for future researchers to work in the field of data security. Based on the outcomes, data security companies and agencies can guide end users, stakeholders and all other people who are involved who are always worried about the security of data [22].

IoT is a world where exchange of data is done between machine to machine and human to machine and vice versa. ISO stands for International Organization for Standardization said about IoT is an Infrastructure of several interconnected devices, objects, people, information systems, application software's that work together physically and virtually and react according to the instructions or input received from one another [23]. Two computing units works hand on hand one is cloud computing and other is IoT. There are two views what IoT does. First one is a set of services it does based on the input received with the help of Internet, and the second one is to do job smartly by using sensors [24].

1.4 Architecture of IoT

As popularity of IoT devices grown up it is adapted by several business units and house. Still there is no single standardized and well-defined architecture of IoT exists. Number of layers may get different in different IoT devices due to their complexity. Architecture of IoT consist of several components like sensors, actuators, protocols, networking system and cloud services [25]. Architecture of IoT is mainly divided into four layers that is required for proper management, it is generally used by admin department in charge to evaluate the system, to monitor the device and to maintain the connectivity of the entire system. IoT architecture have four layers where the data flows from sensors to networks and then to cloud for data processing, analysis and storage [26]. The most common and widely accepted four-layer architecture of IoT is shown the below figure.

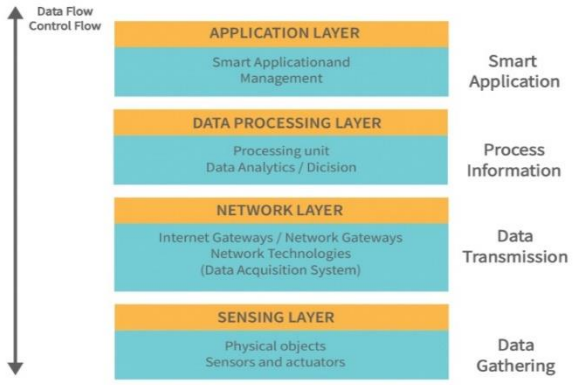


Fig 2: Architecture of IoT

The working of four layers are as follows:

Sensing Layer : First layer of IoT architecture is sensing layer which is responsible for data collection from various resources. This layer mainly consists of two components one is sensor and another one is actuator, these components present in the environment and are responsible for collecting data about light, temperature, sound, humidity, moisture and other parameters [27]. These components are connected to network layer with the help of wireless or wired Internet.

Network Layer: Second Layer is Network Layer which is responsible for establishment of communication system between the IoT devices. It mainly consist of communication protocols and technologies which makes IoT devices to communicate with one another and also communication with cloud for data storage and data analysis [28]. Examples of network layer are Wi-Fi, Bluetooth, mobile network 4G & 5G. This layer also includes routers and gateways to connect IoT devices and Internet. This layer also provides encryption and decryption services for data security.

Data Processing Layer : Third layer of IoT architecture is data processing layer which is responsible for data collection, summarizing and interpretation of the data received from the IoT devices [29]. Data processing layer receives raw data from device, apply formulas to process it and present the information for further analysis for action. This layer mainly consists of database management systems, several algorithms to perform data analysis, these tools helps in obtaining meaningful information from the received data, so that a fruitful decision can be made [30]. Data lake is an example of a technology which works at data processing layer and it stores raw data received from IoT devices and products.

Application Layer: Forth layer or top layer of IoT architecture is application layer. This layer deals with user directly. This layer provides an interface by using which user can control the behavior of IoT device [31]. This layer is accessible using mobile application, website and other user interfaces which ultimately interacts with IoT devices. This layer uses data provided by data processing layer and can apply machine learning algorithms, data visualization etc.

1.5 Architecture of 5G Network

5G network architecture is made up of several service-based components that's why it is also called service-based architecture 5G [32]. The following diagram shows the various components of the architecture [33]:

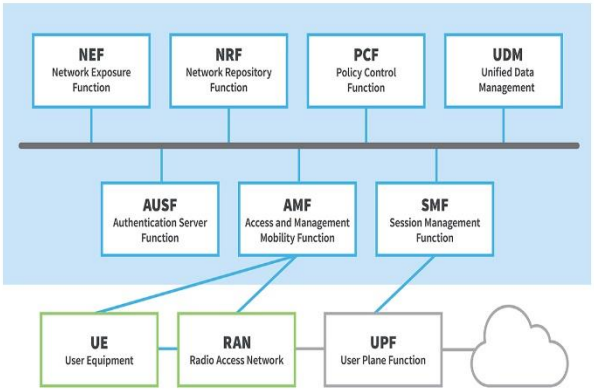


Fig 3: Architecture of 5G Network

Functionality of various components of architecture is as follows:

- UE – User Equipment: here equipment refers to 5G mobile phones or other 5G enabled devices that establishes connection with RAN – Radio Access Network and then connects to DN – Data Network.
- AMF – Access and Management Mobility Function, it acts as a entry point to 5G enabled UE.
- SMF – Session Management Function: depending upon the services demanded by UE; AMF selects the SMF to manage the corresponding session.
- UPF - User Plane Function: this component is responsible for transferring the data over IP between UE and other external network.
- AUSF – Authentication Server Function: This component sets permission to allow AMF to check the authenticity of UE, so that UE can access the services of 5G Network.

- PCF - Policy control Function: this component is responsible for maintain the policies that govern the usage of the network.
- UDM – Unified Data Management: this component is responsible for managing the data of the network.
- Application Function: this component manages the subscription information of the Network.

In the real 5G network is much more complex than the figure discussed, but this complexity needed to provide better service to clients.

2. Literature Review

[34] have proposed intrusion detection system based on gaming theory, it is a combination of signature and anomaly detection techniques for IoT environment. Anomaly detection system starts responding as soon as a new attack is occurred, it is highly beneficial for low power devices. The proposed system creates game model for each user weather it is a authorized user or attacker, based on Nash Equilibrium. Nash Equilibrium is a situation in a game where the user can't move further ahead, instead the user have to change his path. As soon as game model is created, anomaly detection system starts functioning. The system starts observing the network traffic and if any unexpected behavior found it sends warning to the security personnel and alert the system to further diagnose. Since the proposed system is based on a gaming model it can defense from a set of attacking sequence, the system is not ready to provide protection from the attacks coming from the dynamic environment of IoT. The advantages of the proposed system are as follows:

- It has the learning capability to detect new threats.
- It can work on low power devices.

Since the proposed system is based on gaming-based IDS, to improve the performance of the system it could be developed on the concept of dynamic game model. This can be achieved by using machine learning algorithms which will make the system more dynamic, in this manner the defensive system will be able to deal with real time data. One more way to improve the system by using it with the help of other security measurement techniques like firewall, antivirus and access control system.

[35] have developed an anomaly detection system based on Fog in order to secure IoT devices. The proposed system has brought the fog computing technique closure to the edge of the network to detect any anomaly in the IoT devices. Advantages of the proposed system are as follows:

- Reduced Latency: Anomaly detection system based on Fog find out any anomaly faster in comparison to cloud as this system does not have to send data to cloud. It performs calculation at the edge of network which is require by IoT devices to perform operations on real time data.
- Reduced bandwidth requirements: As Fog based anomaly detection system send less data to the cloud, in this manner it saves the bandwidth of network.
- Enhanced scalability: The proposed system is more scalable as it shares the work load on multiple fog nodes, this feature is important in IoT devices which generates more data.

Performance of the proposed system is good in comparison to existing system but there exists no support to continuous learning. Since IoT devices faces new attacks every day, hence the proposed system must have feature of automatic learning, so that in feature any new attack or threat appears, the system must be able to deal with it. Methods to improve the system are as follows:

- Use of Machine Learning Algorithms: The ML Algorithm will train the exiting system about the latest threat pattern of data and if the system is online, it will automatically update about the latest threats.
- Use of Federated Learning Algorithm: This algorithm allows multiple fog nodes uses a system where all nodes do not need to share their data among each other, this is required where data security is a prime concern.

[36] have proposed a method for detection of threat in IoT, this method is based on deep learning and fog computing. Proposed method working is similar to client server architecture, in which distributed fog nodes provides training to a model to detect attacks. The main limitation of this method is that it uses backpropagation based stochastic technique to update the weight gradually. This method of training the model takes longer time which is certainly a limitation for dynamic IoT environment. Compared to previous version of the threat detection system, there are several advantages of the proposed ones are as follows:

- Faster detection: Proposed method uses fog computing which works faster in detection of attacks, fog nodes are available at the edge of the network, hence they do analysis faster and raise alert if any attack found.

- Use of OS-ELM: OS-ELM is one of the efficient model training algorithms, which is required for real time analysis of data received by IoT.

[37] have proposed a method to generate predictions of worm attack. In this method real time analysis is done over the data of network traffic to predict any worm attack. The prediction of the attack is calculated with the help of linear regression and time series formula. The results have shown that the worm prediction success rate is better than the previous methods, the only limitation of the method it can be useful for worm detection not for any other type attack.

[38] have studied a series of attack projection frameworks to develop an understanding of attack strategy changing over time. They proposed a model based on their findings that predicts the next attack, depending on the various types of attack that has been traced in the past. This attack projection work extracts footprints from multistage attacks, with the help of these footprints they were able to create a strategy to find the next attack. The next attack is predicted in this manner, but extracting footprints for a huge network is certainly a challenging task.

[39] have studied several prediction methods on loss of power supply in smart grids. They have used ANN – Artificial Neural Network to generate predictions based on the data collected from several parts of the smart grid, with the help of this data a map is created that will help in generating predictions of the upcoming power failure. They make the computer to understand the map with the help of ANN. However, it was not an easy process to teach the computer as several data is collected from smart grid and the process is complex in nature and the results generated by the system works for some specific conditions only. In today's scenario Distribute Gaussian Regression is used on fog nodes, using this technique predictions of attacks over IoT devices is predicted, it also performs calculations over the real time generated data, in this manner smart grid serves better.

[40] have studied several action selection models and has given their view on the same. There is always a possibility of attack on IoT devices, hence only identification of attack will not be an effective way to get out of the problem, but there must be have a procedure to get out of the situation while maintaining security of data. There are mainly two types of action selection models are there, one is static action selection model and another one is dynamic action selection model. In static action selection model when an attack is detected, manual approach is used to find out which action will resolve the issues while in dynamic action selection model, no intervention of any human is required, the system will identify the pattern of attack and will automatically choose the best possible predefined action. It is found that the IoT environment is highly dynamic in nature and exchange huge amount of data as a result of this it can only dependent on dynamic action selection model only.

[41] have developed an automated action selection model named as AIRS – Automated Intrusion Response System. The proposed system uses a set of values for an action matrix, the output of the matrix will decide which action should be used to neutralize the attack. The limitation of the system is that it is difficult to update rules for choosing of proper action selection model.

[42] have developed an automatic action selection model based on the concept of a series of steps similar to game theory. In this theory the automated action selection is based on a multiplayer game Stackelberg stochastic. The main aim behind the use of this game theory was to making the choosing the best action selection model could be fast and the limitation of the system is that a gaming model is based on a series of action it could not deal with the situations that may occurs in runtime environment of IoT.

[43] have studied several security issues of IoT and have found that none of the solutions found to be useful in each and every case. They have thrown light on the ecosystem of IoT which consists of Communication technology, operational technology & IT. With the help of IoT applications, the ecosystem is able to establish communication between machines and devices. Growth of IoT devices and Internet all over the world became a threat for users' data, data is facing attack from hackers. They have found that the present network communication system does not focus on the security standards of IoT. The study found the security areas that can be improved. They have proposed and implemented security features in 5G network and found that the new applied security measures improved security a lot.

[44] have raised issues that are associated with 5G enabled IoT devices. This communication environment is highly exposed to various security, privacy threats and attack. The researchers have discussed several security protocols and have proposed the way to choose the best one. The findings of this research are as follows:

- Explored various IoT 5G models that are required a communication environment.
- Addition of details related to security and possible attacks that may arise in IoT 5G environment.
- Use of various security protocols.
- Experimental analysis and comparative study of the results is done with existing security protocols and it is found that the proposed security model works better than the existing ones.
- They have also given future research directions and upcoming challenges in the IoT environment.

[45] have proposed IPv6 connectivity with IoT as this technology is growing on a rapid rate. Now IoT is becoming part of everyone's life as it is part of several objects, like IoT is used in appliances, vehicles, television, farming fields etc. these all things becoming smarter and well connected. The growth of IoT get boosted with the help of 5G Network because of its faster communication takes place and with this tremendous growth several challenges also came. One of the main challenges is data security and privacy as IoT devices are becoming part of manufacturing industry, healthcare and also in armed forces. As IoT is development is going on it is becoming complex and several threats and attacks becoming a common, now a days. Hence it become necessary to protect this system and also to make sure that it performs well. To overcome this challenge, they have used nature motivated algorithms as to provide data security and privacy to the system. They have examined security and privacy related issues at network layer of IoT 5G environment. They have done a through literature review regarding security and privacy issues of network layer and at the last they have shared the idea of using bio inspired algorithms to secure the data at network layer in IoT applications while using 5G network.

[46] have studied several security protocols that are part of IoT 5G. The communication system does more than establishing communication between people, it also provides connection and management of various machineries and IoT devices. IoT in integration with 5G provides several applications in the field of remote surgery, smart vehicles, VR cinema, smart home, smart agriculture and smart surveillance system. Although this interconnected system of several devices and users gets interacted with the help of internet but there exists several threat, attacks and privacy related in this environment. The challenge in this era of IoT is to protect data against such threats. Several researchers have developed several security protocol and algorithms in the areas like intrusion detection, public and private key management, encryption and decryption algorithms, access control and device authentication. The authors have provided detailed study of several security protocols to minimize these risks and attacks. In this paper the authors have perform result analysis and comparison of security measures adopted by IoT 5G communication devices. The paper also focuses on the future directions to enhance the security related issues of IoT 5G.

2.1 Simulation Tools

A simulator is a combination of hardware and software, it is a tool which creates a virtual environment to test any model or algorithm before making it available for the real world. It is used in several fields like engineering, manufacturing, production plant, education, research and entertainment. The main use of simulator is to provide a safe and cheaper way to perform experiment in a controlled environment. It certainly minimizes risks and safe also before actually start of any manufacturing of product.

There are several advantages and applications of a simulator which are listed as below:

- Replica of Real World: Simulators copy the behavior of large machineries such as industrial machines, vehicles, railway engines, fighter planes. Simulators uses algorithms and mathematical models to provide similar behavior as of real machines.
- Training and Skill Development: Simulators provide training environment to beginners to enhance skills before using actual machines because there exist several risks on using real machines, hence simulators provide training and skills development. For example, before using the actual fighter plane, pilot learn to use the plane with the help of simulator and after getting proper skills set the pilot starts training on the real plane, in such a manner it is very useful in nature.
- Research and Experiments: Simulators provides a great way to perform research and experiments. It allows to perform experiment and research work on a very low budget, many times it is not feasible to purchase real machines and devices but at a low cost, it is easy to perform experiment on simulator.
- Validation and Testing: scientific experiments are firstly performed on simulators to check whether the

proposed algorithm or design is correct or not, it means validation and testing of the proposed system and model is done with the help of simulator.

- Gaming and Entertainment: Simulators are also being used by Gaming and Entertainment based companies. To provide smart gaming experience, concept of the game is first implemented on simulator, car or motorcycle gaming experience.
- VR – Virtual Reality and AR – Augmented Reality: to deliver smoothing experience now a days AR and VR projects are firstly being tested on simulators before the development of the real product.
- Environmental Modeling: simulators are used to predict the nature of climatic systems.
- Training for Emergency Situation: Simulators are also to provide training to police officers, doctors and defense team, so that they can have an experience to deal with such drastic situations.

Complexity of various simulators are different in nature, for example simulators used for education purpose is less complex and, on another hand, simulators used for effective management of nuclear plant is highly complex in nature. Which simulator is best in which condition it depends on the goal to be achieved and the quality of task to be performed. There is no doubt at all that simulators play an important role in improving safety, security and performance enhancement, it is being used in several areas.

There are several offline and online simulators available to test the security of data in IoT. Some simulators are having GUI and some works on console mode only. Testing of algorithms and models developed for IoT 5G can be easily checkout their performance at network layer of IoT. No need to manage the hardware and software configuration details in depth. Simulators can generate the performance analysis report of the proposed algorithm, the time taken to complete encryption and decryption as well as the time taken to generate keys to perform. RSA is one of the most popular and secured algorithms used to perform encryption and decryption of data. It is a asymmetric key based algorithm, which uses two keys, it means one key is public and another key is private in nature. Public key is used to perform encryption by the sender while receiver uses his private key to perform decryption of the received encrypted data.

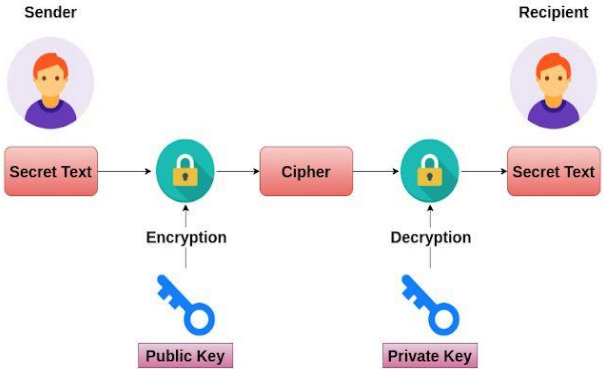


Fig 4: Asymmetric Key Cryptography

2.2 Devglan Simulator

It is a online simulator, which allows to generate public & private key of size 515, 1024, 2048, 3072 and 4096 bit. It uses the generated keys to perform encryption and decryption.

Generate RSA Key Pair button is used to generate public and private keys in this online simulator. Both keys are copied at this step and further it will be used to perform encryption and decryption.

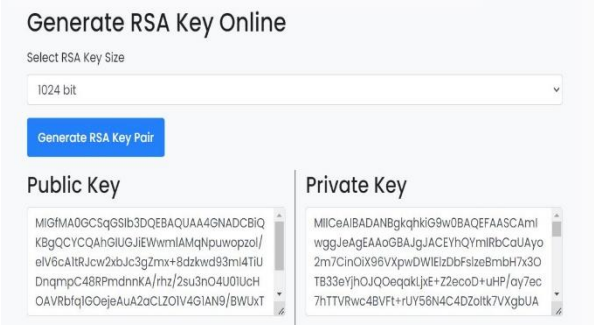


Fig 2.4: Key Generation in Devglan

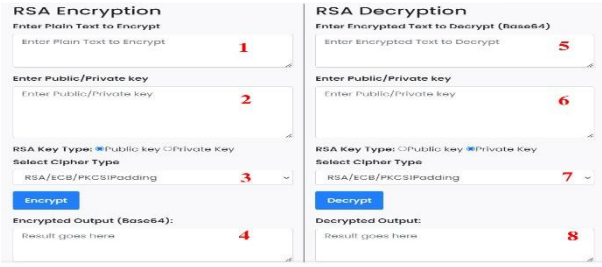


Fig 5: Overview of Devglan

Above figure is numberd from 1 to 8, now lets explore the working mechanism of this simulaor in the following section:

1. In ‘Mark 1’ plain text is written which is to be encrypted.
2. In ‘Mark 2’ public key is pasted which is availabe in the option Generate key online.
3. In ‘Mark 3’ select cipher type there are three options

availabe, any one can be choosen as per the requirement.

4. On click of Encrypt button, encrypted text will be availabe in ‘Mark 4’.
5. To decrypt the encrypted text is copied from ‘Mark 4’ and pasted in ‘Mark 5’.
6. In ‘Mark 6’ private key is pasted which is availabe in the option Generate key online.
7. In ‘Mark 7’ select cipher type there are three options availabe, any one can be choosen as per the requirement to decrypt the encrpted text.
8. On click at Decrypt button the encrypted text at ‘Mark 5’ will be converted back to the original text, the decrypted text will be availabe at ‘Mark 8’.

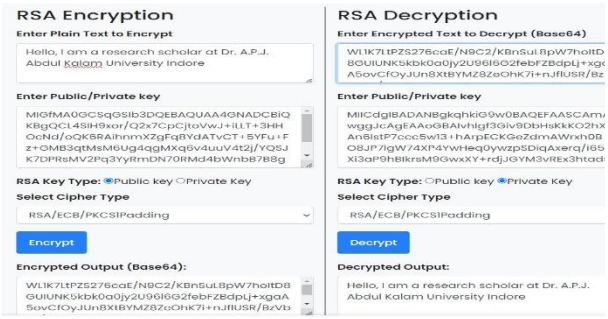


Fig 6: Encryption and Decryption using Devglan

A text “Hello, I am a research scholar at Dr. A.P.J. Abdul Kalam University Indore” is encrypted and decrypted using the simulator.

2.3 JSEncrypt Simulator

JSEncrypt is an online simulator which provides more functionality than the Devglan. This simulator generates private key, public key and performs encryptiona and decryption using several modified RSA techniques. It generates keys of sizes 512, 1024, 2048, 3072 and 4096 bit.

Fig 7: Key Generation in JSEncrypt

In the above figure public and private keys are generated of size 1024 bit, to perform this operation Generate Keys button is used. In the following figure encryption is performed of the text “Hello, I am a research scholar at Dr. A.P.J. Abdul Kalam University Indore”. In the first texbox plain text is written and in the second texbox public key is pasted from the Key Generation screen. This simulator offers six different types of encryption methods to encrypt the data, depending on the requirenent best option can be choosen. On click of Encrypt button plain text will be encrypted.

Fig 8: Encryption using JSEncrypt

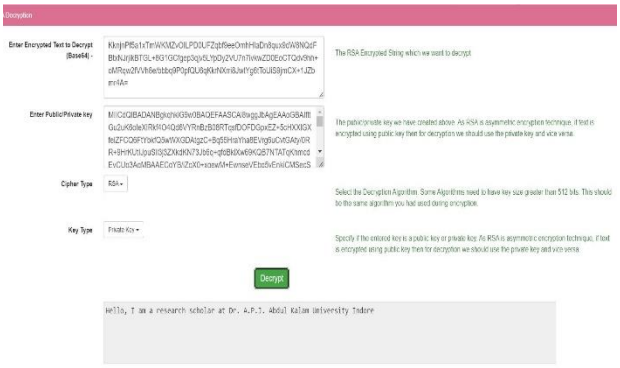


Fig 9: Decryption using JSEncrypt

To perform decryption, encrypted text is pasted in first textbox. In second textbox private key is pasted from key generation screen. It performs decryption using six different techniques. On click of Decrypt button, original plain text will be back in the textbox below the Decrypt button. In this manner it performs encryption, decryption and generates keys.

3. Proposed Solution

Data security issues can be resolved by using RSA asymmetric key cryptography. It has also been found that RSA algorithm has certain limitations. In this chapter following tasks will be performed to achieve data security goals for IoT-5G.

- Boltzmann Machine is used to generate secured keys. Its performance will be compared with other methods to generate keys, encryption and decryption time.

- Performance Enhancement of RSA algorithm will be done and further it's performance will be compared with existing versions of RSA.

Above task will enhance the secured key generation process using machine learning algorithm, Encryption and Decryption Process of RSA in order to provide data security at Network Layer of IoT-5G.

3.1 Boltzmann Machine for Generating secured keys for IoT-5G Devices

In 1980s, Boltzmann Machine was developed by Terry Sejnowski and Geoffery Hinton, it is one of the most popular artificial neural networks. The name Boltzmann Machine is given on the name of Austrian Physicist and Scientist Ludwig Boltzmann, he is known for his extraordinary contributions in the field of statistical mechanics. Boltzmann Machine is a probabilistic neural network, it is used for unsupervised learning and it can be used to perform several tasks related to machine learning for example recommendation system, feature learning & intrusion detection system etc. [223].

Following are the properties of Boltzmann Machine [224]:

- Nodes: Boltzmann Machine is form of several Nodes. Nodes can be considered as artificial neurons, these nodes forms layer. Layers are of two types one is visible and another is hidden.
- Connectivity: Nodes present at different layers are well connected with each other, it means that each visible node is connected with hidden node and vice versa. The nodes present on the same layer are not connected with each other.
- Energy Function: To measure the compatibility among hidden and visible nodes an energy function is used in this machine. The energy functions is used to configure the network by providing energy value.
- Stochasticity: Nature of Boltzmann Machines are stochastic, to model data it uses probabilistic approach.
- Learning: In order to minimize the energy of network configuration, the weight of the connections established between the nodes is minimized while training a Boltzmann Machines.

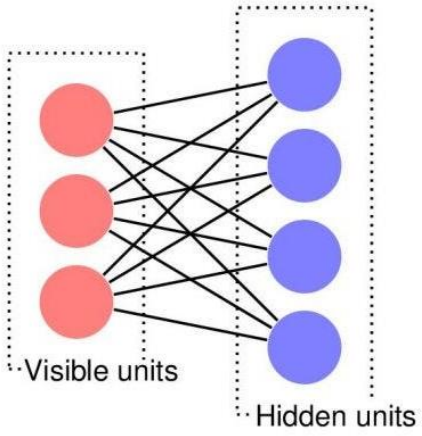


Fig 10: Visible Nodes and Hidden Nodes of BM Machine

During the earlier days of Boltzmann Machines, it was a tough task to train the machine because of computation complexity but there after several simplified versions of Boltzmann Macines came into existence like Restricted Boltzmann Machines – RBM, Deep Boltzmann Machine – DBM. The new and modified versions of the Boltzmann Machines are highly effective and more practical oriented in nature [225].

In the upcoming section, of the paper aim is to develop a method to generate secured keys for IoT-5G enabled devices using Restricted Boltzmann Machines. Deep Learning based Restricted Boltzmann Machine Algorithm will provide a more dynamic, robust and efficient key generation process will be formed. Restricted Boltzmann Machine have been provided through training and evaluation has been done in order to check the flexibility of the proposed systems encryption process. The main objectives behind the development of the proposed key generation using Restricted Boltzmann Machine are as follows:

- Mutual Authentication: During data handover each device must authenticate each other.
- Privacy: During the exchange of data among the device's identity of IoT 5G devices should not be disclosed.
- Session Key Exchange: Exchange of session keys should be done and the security of session keys should not be compromised.
- Defense against attack: it must generate the capability of defensing against with the aim to provide data security and device protection.

There are two types of nodes present in the Restricted

Boltzmann Machine, they are different from each other but Boltzmann considers it as one system. Dataset to train the proposed key generation method is downloaded from Kaggle, Restricted Boltzmann Machine adjust the weights of the data according to the requirement. The system works well in normal conditions and is helpful in dealing with the attack if occurred. Restricted Boltzmann Machine generates various states of machine that depends on the conditions of the system. As energy of the system increases, there exists lesser chances of the system being in ground state. It is found that the value of state level is inversely proportional to value energy level, it means as state level increases energy level decreases and if energy level increases value of state level decreases. Restricted Boltzmann Machine distribution is used to generate secured cryptographic key by using the modified formula as follows.

$$P_i = \frac{e^{(-\varepsilon_i/KT)}}{\sum e^{(-\varepsilon_j/KT)}} - \left(\sum_{i<j} w_{ij}\, S_i\, S_j + \sum_i \theta_i S_i \right) \ldots\ldots\ldots (1)$$

$$P_i = \frac{\emptyset e^{(-\varepsilon_i/KT)}}{\sum e^{(-\varepsilon_j/KT)}} - \left(\sum_{i<j} w_{ij}\, S_i\, S_j \right) \ldots\ldots\ldots (2)$$

In the above proposed formula P_i refers to the probability of a system present in *i* state, T refers to temperature of system, k refers to Boltzmann constant, $\Sigma e^{(-\varepsilon/kT)}$ refers to all possible states of system. Equation (1) will be used in performing encryption of message while equation (2) will be used in performing decryption.

$E(visible\_nodes, hidden\_nodes) = -\Sigma a_i(visible\_nodes_i) - \Sigma b_i(hidden\_nodes_j) - \Sigma(visible\_nodes_i * w_{ij} * hidden\_nodes_j)$

In this manner the Restricted Boltzmann Machine is came closure to the dataset of contrast divergence, it determines the specifications and features that are required to complete the training process. In our system predicts the session key performance in encryption of data it will perform good, bad based on the performance of the previous result. On the basis of weather, the encryption method works (good – 1), (bad – 0) and empty dataset must be occupied by 0, 1 or the row must be deleted.

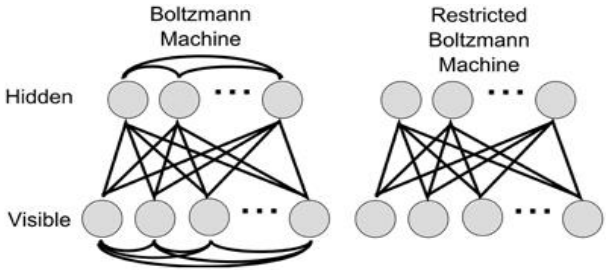


Fig 11: Working of BM and Restricted BM

Contrastive Divergence:

The main task of Restricted Boltzmann Machine - RBM is to adjust the weights. RBM uses weighing methods which is similar to assignment of some random initial weights to the input nodes. The hidden nodes is form of all nodes and the visible node form with the help of hidden nodes. Although the weights are same but the input is different of each other. This process continues till the new input weights became same as the previous ones. This procedure of repeating the weights is known as Gibbs sampling. Hidden nodes do not connect with other hidden nodes while in the same manner visible nodes also does not connect each other. The proposed methodology efficiently trains a multilayer and well-connected model.

In the proposed approach a dynamic and more functional asymmetric key generator is generated using RBM. This joint use of RBM does perform encryption of plain text and decryption of encrypted text. To demonstrate the systems usability, its time to conduct a security analysis. During the process of encryption and decryption each character is changed. The eight neurons output is masked in a single layer, which is responsible for encryption of various sets of eight-bit input.

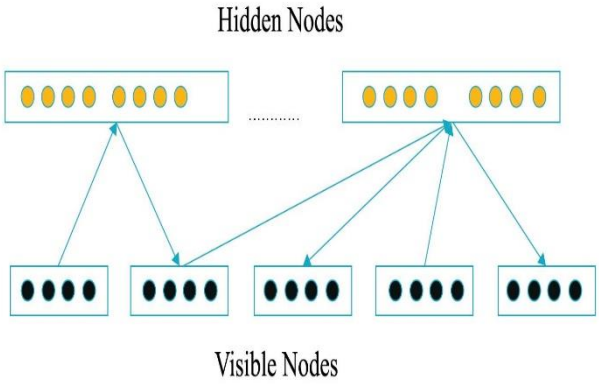


Fig 12: Working of Hidden nodes and Visible Nodes

Output of the hidden layer will be a floating-point value as the activation function of the hidden layer falls in the range of 0 to 1. Hence eight-dimensional

vector have the encrypted text, it represents an array of floating-point values of eight length in multiplication to the given input data.

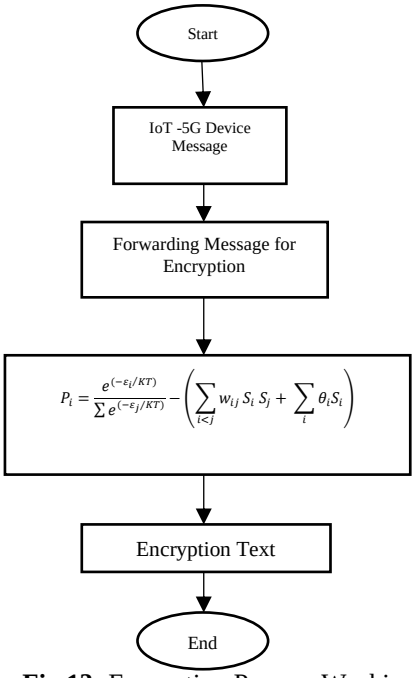
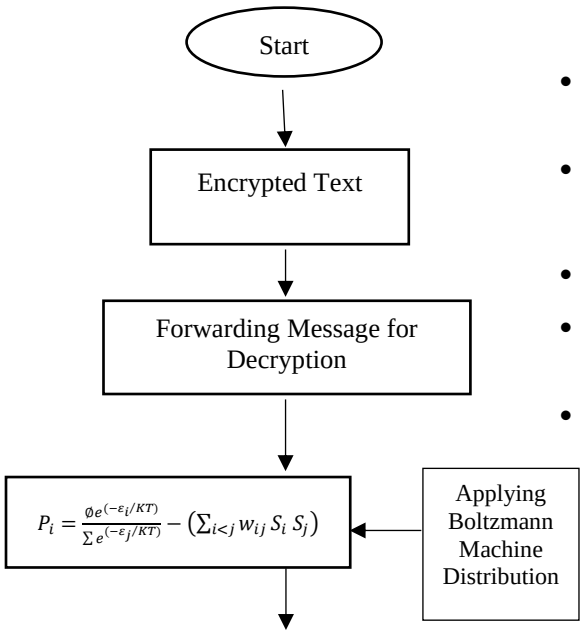


Fig 13: Encryption Process Working.

Output layer consist of floating-point numbers, twelve-dimensional floating number vector will process decryption of the text using the Boltzmann Machine Distribution function along with the proposed formula the original text will be generated.



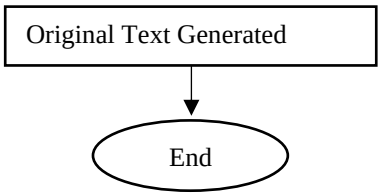


Fig 14: Decryption Process Working

3.2 Modified RSA for Generating secured keys, encryption and Decryption for IoT-5G Devices

To improve the security standards of RSA while maintaining performance of core RSA [47], a modified version of RSA is proposed and implemented that uses five distinct prime numbers.

Proposed Method of Key Generation:

- Start
- Choosing five different prime numbers p, r, i, m and e.
- Perform modulus, product = (p * r * i * m * e).
- Calculation of Eulers totient function φ (product) = [(p-1) * (r-1) * (i-1) * (m-1) * (e-1)]
- Generation of two different prime numbers A1 and A2 with the help of prime number generator, make sure that A1 and A2 are not cofactors of φ (product).
- Perform Z =[|NextPrimeNumber(A1+2)-A2|] % product.
- Calculation of the public key PublicKey such that it is coprime of Z and φ (product).
- Calculation of private key PrivateKey in such a manner (PublicKey * PrivateKey) % (φ (product) * Z) must be equal to 1.
- Perform N = NextPrimeNumber(p*r*m) * NextPrimeNumber(i*e).
- End

Proposed Method of RSA Encryption:

- Start
- Calculation of Encrypted Message EM = (OriginalMessage^ PublicKey) % N.
- End

Proposed Method of RSA Decryption:

Start

- Generating Original Message OM = (EM^ PrivateKey)%N
- End

4. Implement

To implement the proposed RSA following configuration of hardware and software is used: -

Hardware of the Computer System:

- Hard Disk Drive: 1 TB
- RAM: 8GB
- CPU: i3

Software of the Computer System:

- Programming Language Used: Python
- Application Software: Notepad++
- Operating System: Windows 10

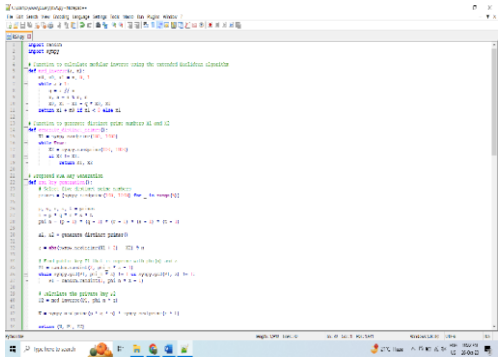


Fig 15: Modified Key Generation in Modified RSA

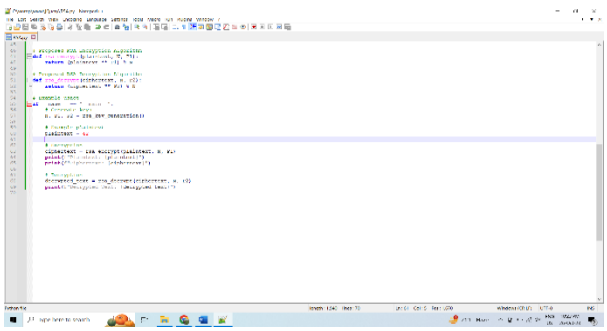


Fig 16: Encryption & Decryption in Modified RSA

Above screenshots are of the program developed in Python for the proposed algorithm of Modified Key generation, encryption and decryption of RSA. The results and its performance analysis are done in next chapter.

5. Result Analysis

In this section, results of the developed programs will be discussed and in order to measure the performance of the proposed algorithms comparative study will be done.

5.1 Result Analysis of Proposed Secured key Generation, Encryption and Decryption using Boltzmann Machine

In this section results are shared of the proposed secured key generation, encryption and decryption using Boltzmann Machine is discussed and analyzed. To analyze the performance and results following parameters have been taken into consideration.

- Key Generation Time: it refers to the overall time taken to generate keys to encrypt and decrypt data. Key generation time should be less, so that further process of encryption and decryption can takes place.
- Encryption Time: it refers to the overall time taken from starting of encryption process and completion of encryption process. This time should be less, lesser the time taken by the algorithm shows more the performance.
- Decryption Time: it refers to the overall time taken from the starting of decryption and completion of decryption. Lesser the time to complete the decryption of encrypted text shows more the performance.

A set of data files is created of various sizes 600KB, 800KB, 6MB, 12MB, 40 MB, 100MB and 150MB developed. These dataset files will be encrypted and decrypted using the program developed in Python language, timeit module of Python is used to calculate the time taken to complete the encryption and decryption of each file using the same proposed method and formula.

In Python, timeit() function of timeit module return time in seconds, since most of the results are in less than one second and answers are in decimals, to present the answers in more simplified manner, answers are converted into milliseconds by multiplying with one thousand.

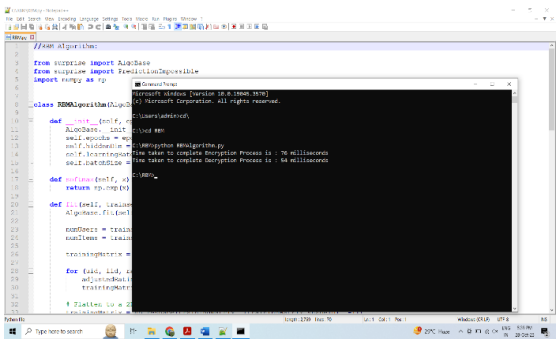


Fig 17. Encryption and Decryption Time

The above screenshot of the program does encryption and decryption of 600 KB data file with the help of proposed program. Time taken to complete the encryption and decryption process is 76 and 54 milliseconds. To get the more accurate time each time a single file is encrypted and decrypted fifteen time and the average time calculated and noted down.

In the similar manner encryption and decryption of other datasets file completed and the time taken by the proposed algorithm to complete the encryption and decryption process is shown in the below table.

Table 1. Encryption and Decryption Time of all Files

File Input Size	Encryption Time take by the proposed method and formula	Decryption Time take by the proposed method and formula
600 KB	76	54
800 KB	100	80
6 MB	150	120
12 MB	300	220
40 MB	500	420
100 MB	600	510
150 MB	926	813

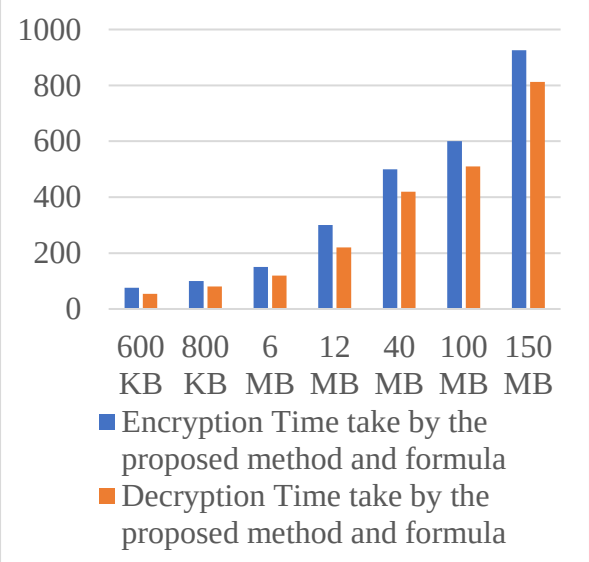


Fig 18. Encryption and Decryption Time by the proposed work

From the above Table 1 & Figure 18, it is found that Encryption Method takes more time in comparsion to decryption of data. Now further a compartaive study will be done in oder to compare the performance of the proposed methodology and formula with Diffie-Hellman [48], RSA [49], ECC [50], ECDH [51]. Performance will be measured on the total amount of time taken to encrypt and decrypt a file of same sizes as in the above table 600 KB, 800 KB, 6 MB, 12 MB, 40 MB, 40 MB, 100 MB, 150 MB.

Table 2: Analysis of encryption time of proposed work with others

File Input Size	Encryption Time take by the proposed method and formula	Diffie-Hellman	RSA	ECC	ECDH
600 KB	76	246	243	228	236
800 KB	100	370	377	288	350
6 MB	150	388	570	298	359
12 MB	300	398	588	399	568
40 MB	500	588	656	596	636
100 MB	600	687	745	688	689
150 MB	926	1023	1021	940	935

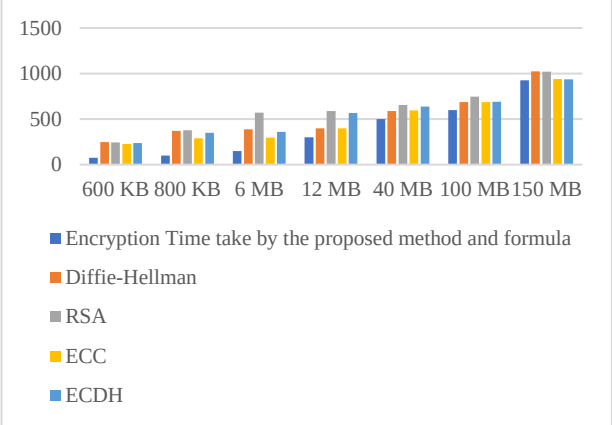


Fig 19: Comparison of encryption time of proposed work with others

In the above Table 2 & Figure 19, it is found that the time taken by the proposed method and formula takes lesser time to encrypt data in comparison to other methods. It shows that the performance of the proposed work is better under various input of different file size.

Table 3: Analysis of decryption time of proposed work with others

File Input Size	Decryption Time take by the proposed method and formula	Diffie-Hellman	RSA	ECC	ECDH
600 KB	54	86	198	98	93
800 KB	80	275	290	190	198
6 MB	120	296	298	199	298
12 MB	220	298	480	470	460
40 MB	420	432	498	489	499
100 MB	510	552	510	599	632
150 MB	813	853	898	802	898

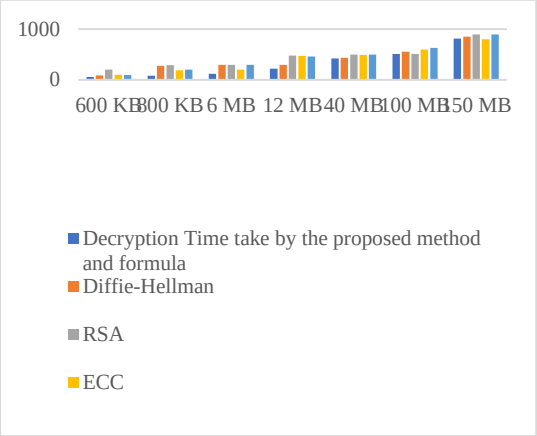


Fig 20: Comparison of decryption time of proposed work with others

From the above Table 3 & Figure 20 it is found that the time taken by the proposed method and formula takes lesser time to decrypt data in comparison to other methods. It shows that the performance of the proposed work is better under various input of different file size.

Thus, from the above Table 2 & Table 3 it can be calculated that the performance of proposed work during encryption & decryption of data is better than the traditional approach.

5.2 Result Analysis of Proposed RSA for Encryption and Decryption of data

Message: "Hello I am a research scholar" is used to encrypt and decrypt to evaluate the performance of Proposed RSA. The output of the program appears as follows:

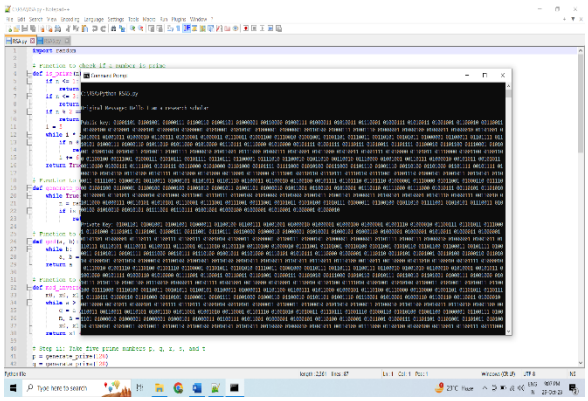


Fig 21: Output of the proposed RSA

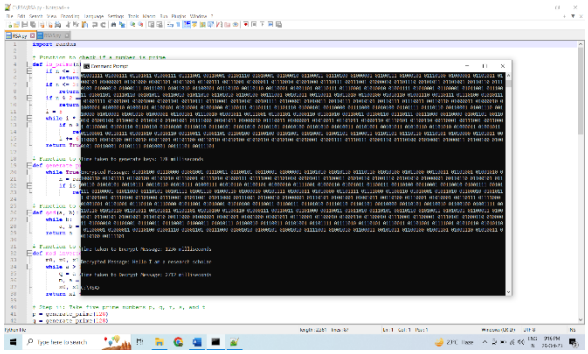


Fig 22: Time taken to complete encryption and decryption time

Table 4: Time consumption by the Proposed RSA

Time taken by the Proposed RSA to perform the task:	
Time taken to generate keys	178 milliseconds
Time taken to encrypt message	1236 milliseconds
Time taken to decrypt message	2712 milliseconds

The proposed RSA generates public and private keys in 178 milliseconds. It performs encryption of message in 1236 milliseconds, while it decrypts message in 2712 milliseconds. The time mentioned by calculating the average of the program by running it

fifteen times. Program is developed in Python as already mentioned in previous chapter. To measure the time taken to generate keys, encryption and decryption, Python timeit module is used and the function timeit() is used. The accuracy of timeit() is very high. It provides results in milliseconds.

To analyze the performance of the proposed RSA, its performance will be compared with other modified versions of RSA namely HRSA [52], MRSA [53] and R-RSA [54]. The unit of time is milliseconds is used in the below table.

Table 5: Performance analysis of Proposed RSA with others

Name of Modified RSA	Time taken to generate Keys	Time taken to Encrypt Message	Time taken to Decrypt Message	Total Time to Generate Keys, Encryption & Decryption
Proposed RSA	178	1236	2712	4126
HRSA	220	1635	3120	4975
MRSA	210	1582	3526	5318
R-RSA	188	1248	2734	4170

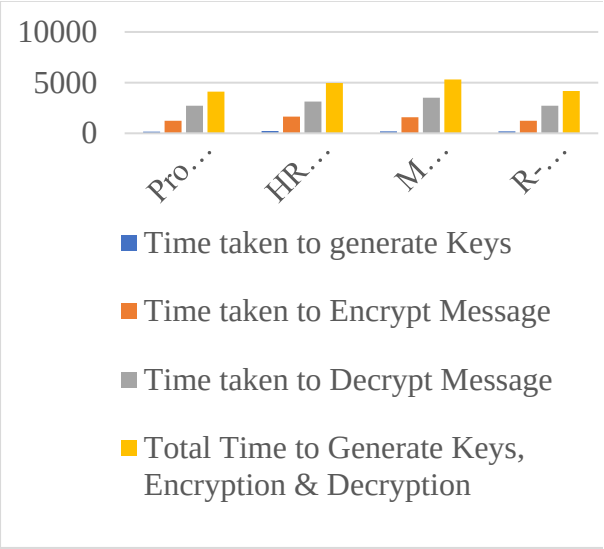


Fig 23: Comparision of Time taken by Proposed RSA and others

From the Table 5 & Figure 23, it is found that the proposed RSA performance is higher than the HRSA, MRSA & R-RSA, following conclusions can be drawn:

- Proposed RSA generates keys in 178 MS, while HRSA, MRSA & R-RSA generates keys in 220 MS,210 MS,188 MS respectively. This means the proposed RSA generates key faster as compare to others.
- Proposed RSA performs encryption in 1236 MS, while HRSA, MRSA & R-RSA performs encryption in 1635 MS,1582 MS, 1248 MS respectively. This means the proposed RSA performs encryption at faster rate.
- Proposed RSA performs decryption in 2712 MS, while HRSA, MRSA & R-RSA performs decryption in 3120 MS,3526 MS, 2734 MS respectively. This means the proposed RSA performs decryption at faster rate.
- Overall, time taken by the proposed RSA (Key generation time, Encryption Time and Decryption Time) is 4126 MS, while HRSA, MRSA & R-RSA takes time 4975 MS, 5318 MS, 4170 MS respectively.

6. Conclusion

This research paper explores the enhancement of data security in IoT-5G networks. It focuses on using the Boltzmann Machine for generating secured keys and improving the RSA algorithm's performance. The methodology includes developing a dynamic and efficient key generation process and applying machine learning algorithms to the encryption and decryption process. The results show that these modifications lead to a more secure, robust, and efficient system for protecting IoT-5G devices, providing a foundation for future research in IoT data security and device protection.

Author contributions

Pratik Shah : Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Validation., Field study. Dr. Deepika Pathak: Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] E. Leloglu, "A Review of Security Concerns in Internet of Things," Journal of Computer and Communications, vol. 5, pp. 121-136, 2017.

[2] J. Singh, T. Pasquier, J. Bacon, H. Ko and D. Eyers, "Twenty Security Considerations for Cloud-supported Internet of Things," IEEE Internet of things Journal, vol. 3, pp. 126-134 2016.

[3] X. Huang, P. Craig and H. Y. Lin, "SecIoT: A Security Framework for the Internet of Things," IEEE Internet of things Journal, vol. 9, pp. 3083-3094, 2015.

[4] M. Mohammadi, M. Aledhari, A. Al-Fuqaha, M. Guizani and M. Ayyash, "Internet of Things: A Survey on Enabling," IEEE Explore, vol. 2, pp. 138-142, 2015.

[5] L. Atzori, A. Iera and G. Morabito, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, pp. no. 3594-3608, 2012.

[6] R. Zejun, L. Xiangang, Y. Runguo and Z. Tao, "Security and privacy on internet of things," in Electronics Information and Emergency Communication (ICEIEC), 7th IEEE International Conference, July 2017, pp. 150-156.

[7] Z. Zhang and Q. Wen, "Application of dynamic variable cipher security certificate in internet of things," in International Conference on Cloud Computing and Intelligent Systems (CCIS), July 2012, pp. 203-209.

[8] K. Zhao and L. Geo, "A survey on the internet of things security," in International Conference on Computational Intelligence and Security (CIS), August – 2013, pp. 663-667.

[9] H. Suo, W. Zou, and C. Liu, "Security in the Internet of Things: A Review," IEEE International Conference on Computer Science and Electronics Engineering, March 2012, pp. 23-25.

[10] T. Nguyen and K. Laurent, "Survey on Secure Communication," Protocols for the Internet of Things. Ad Hoc Networks, vol. 32, pp. 17- 31, 2015.

[11] A. Arseni, S. Halunga, S. Fratu and O. Vulpe, "Analysis of the Security Solutions Implemented in Current Internet of Things Platforms," in IEEE Conference on Grid, Cloud & High Performance Computing in Science, Romania, October 2015, pp. 28-30.

[12] A. Tahir, M. Maier and A. Fernando, "A novel IC Metric based framework for securing the Internet of Things," in IEEE International Conference on Consumer Electronics, August 2016, pp. 469-470.

[13] C. Zhang and C. Liu, "A Novel Approach to IoT Security Based on Immunology," in Ninth International Conference on Computational Intelligence and Security, August 2013, pp. 316-322.

[14] C. Zhou, "Multimedia traffic security architecture for the internet of things," IEEE Explore, vol. 25, pp. 35-40, 2011.

[15] Rose, "Security meets nanoelectronics for Internet of things," in International Great Lakes Symposium on VLSI, May 2016, pp. 356-362.

[16] L. Santos, F. Guimaraes and C. Rodrigues, "A DTLS based security architecture for the Internet of Things," in IEEE Symposium on Computers and Communication, 2015, pp. 482-486.

[17] B. Carminati, E. Ferrari and M. Viviani, "Security and Trust in Online Social Networks," Synthesis Lectures on Information Security, Privacy, and Trust, Vol. 6, pp. 163-172, 2021.

[18] H. Gunasinghe and E. Bertino, "RahasNym: Protecting against Linkability in the Digital Identity Ecosystem," 35th IEEE International Conference on Distributed Computing Systems, USA, June 2015, pp. 365-375.

[19] H. Gunasinghe, A. Kundu, E. Bertino, H. Krawczyk, S. Chari, K. Singh and D. Su, "PrivIdEx: Privacy Preserving and Secure Exchange of Digital Identity Assets," in The World Wide Web Conference, USA, May 2019, pp. 456-461.

[20] A. Barth, A. Datta, J. C. Mitchell and H. Nissenbaum, "Privacy and Contextual Integrity: Framework and Applications," in IEEE Symposium on Security and Privacy, USA, May 2006.

[21] R.V. Nehme, E. A. Rundensteiner and E. Bertino, "A Security Punctuation Framework for Enforcing Access Control on Streaming Data," in 24th International Conference on Data Engineering, Mexico, March 2008, pp. 376-389.

[22] E. Bertino, "Security and Privacy in the IoT," in 13th International Conference Inscrypt China, November 2017, pp. 10726-10732.

[23] E. Bertino, "Data Security and Privacy in the IoT," in 19th International Conference on Extending Database Technology, France, March 2016, pp. 898-912.

[24] J. Sametinger, J. W. Rozenblit, R. L. Lysecky and P. Ott, "Security Challenges for Medical Devices," Communications of ACM, Vol. 58, pp. 74-82, 2015.

[25] J. Valente and A. S. Cardenas, "Security & Privacy in Smart Toys," in International Conference on Internet of Things Security and Privacy, USA, November 2017, pp. 1026-1031.

[26] Y. Shoshitaishvili, R. Wang, C. Hauser, C. Kruegel and G. Vigna, "Firmalice-Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware," in 22nd Annual Network and

Distributed System Security Symposium, USA, February 2015, pp. 236-242.
[27] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, “Deep learning with differential privacy,” in ACM SIGSAC Conference on Computer and Communications Security, March 2016, pp. 308–318.
[28] E. M. Newton, L. Sweeney, and B. Malin, “Preserving privacy by deidentifying
[29] 59. face images,” IEEE transactions on Knowledge and Data Engineering, vol. 17, pp. 232–243, 2005.
[30] K. W. Bowyer, “Face recognition technology: security versus privacy,” IEEE Technology and society magazine, vol. 23, pp. 9–19, 2004.
[31] L. L. Gremillion, “Designing a bloom filter for differential file access,” Communications of the ACM, vol. 25, pp. 600–604, 2021.
[32] L. Tan and N. Wang, “Future internet: The internet of things,” in 3rd International Conference on Advanced Computer Theory and Engineering, 2010, pp. 370–376.
[33] A. Gupta and N. K. Walia, “Cryptography algorithms: A review," International Journal of Engineering Research and Development, 2014, vol. 2, pp. 1667-1672.
[34] J. A. Stankovic, “Research directions for the internet of things,” IEEE Internet of Things Journal, vol. 1, pp. 3–9, 2014.
[35] C. W. Tsai, C. F. Lai, and A. V. Vasilakos, “Future Internet of Things: open issues and challenges,” Wireless Networks, vol. 20, pp. 2201–2217, 2014.
[36] A. Rehash, R. Pavitra, E. Srie, V. Janani, and P. G. Scholar, “Low Delay and High Throughput Data Collection in Wireless Sensor Networks with Mobile Sinks,” International Journal of Scientific Engineering and Research, vol. 8, pp. 589-595, 2017.
[37] J. An, X. Gui, W. Zhang, J. Jiang, and J. Yang, “Research on social relations cognitive model of mobile nodes in Internet of Things,” Journal of Network and Computer Applications, vol. 36, pp. 799–810, 2013.
[38] W. Ji, L. Li, and W. Zhou, “Design and implementation of a RFID Reader/Router in RFID-WSN hybrid system,” Future Internet, vol. 10, pp. 798-810, 2018.
[39] D. He and S. Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,” IEEE Internet of Things Journal, vol. 2, pp. 72–83, 2015.
[40] K. Demestichas, N. Peppes, and T. Alexakis, “Survey on security threats in agricultural IoT and smart farming,” Sensors (Switzerland), vol. 20, pp. 1–17, 2020.
[41] P. R. Lutui, B. Cusack, and G. Maeakafa, “Energy efficiency for IoT devices in home environments,” in IEEE International Conference on Environmental Engineering, June 2018, pp. 1–6.
[42] M. Khosyi‘in, S. A. D. Prasetyowati, Z. Nawawi, and B. Y. Suprapto, “Review and design of GPS-RFID localization for autonomous vehicle navigation,” in ACM International Conference Proceeding Series, Sep. 2019, pp. 42–46.
[43] M. G. Gnoni, V. Elia, and A. Rollo, “RFID technology for an intelligent public transport network management,” International Journal of RF Technologies: Research and Applications, vol. 3, pp. 1–13, 2012.
[44] H. Farhat, P. Iliev, P. Marriage, and N. Rolland, “An added value alternative to RAIN RFID items characterization in retail,” IEEE Access, vol. 6, pp. 32430–32439, 2018.
[45] B. Khoo, “RFID as an enabler of the internet of things: Issues of security and privacy,” in IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing ,2011, pp. 709–712.
[46] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, “A Survey on the Cryptographic Encryption Algorithms,” International Journal of Advanced Computer Science and Applications, vol. 8, pp. 116-124, 2017.
[47] A. Maity, R. Ghosh and S. Bhadra, "Image Encryption Using RSA and Advanced Caesar Cipher Method," in International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India, 2022, pp. 1-5.
[48] I. R. Jeong, J. O. Kwon and D. H. Lee, "Strong Diffie-Hellman-DSA Key Exchange," IEEE Communications Letters, vol. 11, pp. 432-433, 2007.
[49] T. D. Nguyen, T. D. Nguyen and L. D. Tran, "Attacks on Low Private Exponent RSA: An Experimental Study," in 13th International Conference on Computational Science and Its Applications, Ho Chi Minh City, Vietnam, 2013, pp. 162-165.
[50] K. Kwon, D. Kim, S. Park and J. Kim, "EPA ECC: Error-Pattern-Aligned ECC for HBM2E," in International Technical Conference on

Circuits/Systems, Computers, and Communications (ITC-CSCC), Jeju, Korea, Republic of, 2023, pp. 1-6.
[51] R. Sankar, T. Subashri and V. Vaidehi, "Implementation and integration of efficient ECDH key exchanging mechanism in software-based VoIP network," in International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 2011, pp. 124-128.
[52] Qing Liu, Yunfei Li, Lin Hao and Hua Peng, "Two efficient variants of the RSA cryptosystem," International Conference on Computer Design and Applications, Qinhuangdao, 2010, pp. 550-553.
[53] K. Pavani and P. Sriramya, "Enhancing Public Key Cryptography using RSA, RSA-CRT and N-Prime RSA with Multiple Keys," in Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1-6.
[54] A. Karakra and A. Alsadeh, "A-RSA: Augmented RSA," 2016 SAI Computing Conference (SAI), London, UK, 2016, pp. 1016-1023.