RFAS Key Generation to Enhance Authentication and Search in RFID Environments

V. Vishu, R. Manimegalai

Abstract--- *the proposed method unite RFID tag information and sensor values into a 16-bit key to the authentication named as Radio Frequency Authentication Search Key (RFAS), which shows improvement in efficiency. The different strategies used in RFID environment, various parameters in human monitoring systems, classification on encryption techniques, the search techniques with decision making, and the need of optimization techniques. In this paper, the structure of RFAS key and its use in the monitoring scheme is explained. The workflow of RFAS key in monitoring and search inside a jail environment is also presented. Different key generation techniques are compared with RFAS key formation in this work.*

Index Terms--- *Intelligence, Sensors, Radio Frequency Identification Readers and Tags, Smart AES Algorithm.*

I. INFRASTRUCTURE OF THE JAIL ENVIRONMENT

The jail environment is considered as different sections as office area, entertainment areas, work areas, administrator rooms, smoke rooms, inmate’s cell, dining area, kitchen, and parking areas. Four Alien RFID readers are placed in different locations of the jail. Each reader has four antennas; totally, 16 antennas are placed in each entry exit points to different areas to record the movements. The jail has got a leaf structure and two different ways of fencing are done outside. Three office rooms have the central control with administrator room. Tags are attached to the wristband of inmates. Different sensors are placed in surfaces, human body, and electronic devices, which continuously monitor and record the values and used predict human behavior from time to time. The main purpose of this intelligent RFID design of jail is to increase the influence of healthy atmosphere by reducing the occurrences and relentlessness of disruptive behaviors, aggression, pressure and nervousness (Li *et al*., 2002). The automation and recorded data are used as evidence if required. This data are beneficial in mental and social aspects of jail inmates. The typical jail infrastructure considered for this work is shown in Figure 1.1.

The inmates cells are almost at the central part and each entry exit points are enabled with RFID readers and sensors. The primary goal of this intelligent design is making the accused living more efficient and convenient. This system can provide both location tracing and health alarms. Passive RFID tag locates the inmate’s physical- and health-related activities and can also identify the presence of any electronic device. The RFAS key considers the behavioral predictions from sensors and physical movement information from RFID readers and increases the efficiency of the key. The scanned tag values and sensor values are combined to generate RFAS key. The most significant 8-bits are given priority for authentication and updated from the RFID tag vales. The least significant 8-bits are the values received from sensors and classified into different categories such as critical actions, temperature, physical movements, and predicted value based on these.

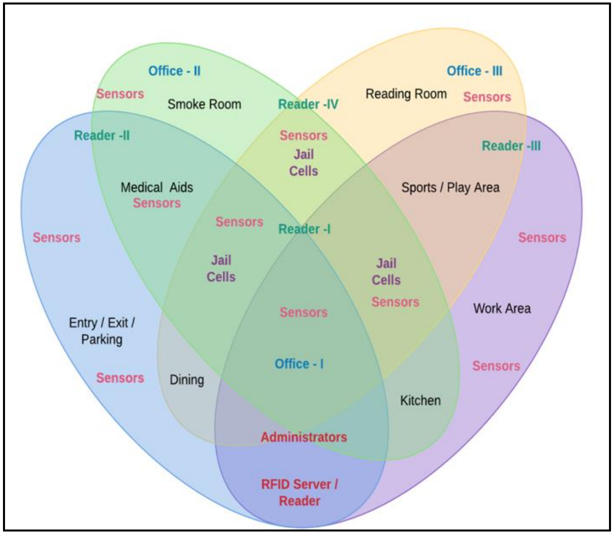
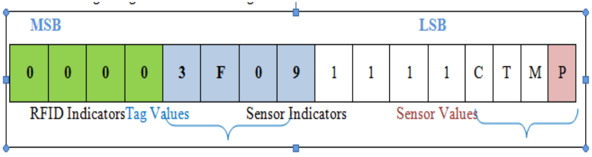


Figure 1.1: Jail Infrastructures with RFID and Sensors

Once the data are collected both from RFID and sensors, need an analysis on the same to create RFAS key. The RFAS key generated is used to enhance the authentication and search algorithms to increase the efficiency in terms of memory usage, speed, and number of transformations in encryption process as well as search. AES and alpha-beta pruning algorithm are taken into consideration with RFAS key for the enhancement. The tag ID is a 16-bit value such as 8000 0100 8820 3F09 and sensors are different variable length depends on health or environmental sensors. The last four bits of tag ID 3F09 is taken and prefixed with four 0’s. Last 8-bit values are the four 1’s and predicted values from intelligent agents as shown in Figure 1.2.



0	0	0	0	3	F	0	9	1	1	1	1	C	T	M	P

Figure 1.2: The Structure of Radio Frequency Authentication Search Key

Manuscript received September 16, 2019.

V. Vishu, Research and Development Centre, Bharathiar University, Coimbatore, T.N, India. (e-mail: vishusabulal@gmail.com)

R. Manimegalai, Research and Development Centre, Bharathiar University, Coimbatore, T.N, India. (e-mail: mmegalai@yahoo.com)

The sensor values represented using C, T, M, and P, which indicates critical actions to be taken, temperature, and physical movement and prediction values. The RFDS combines the movement, environment, and behavioral prediction values to the alpha-beta pruning algorithms.

Preprocessed information such age group, medical histories, and crime category, physical or mental disabilities, and dynamic information from the body attached sensors such as body temperature, walking speed, responding time are combined and predict an 8-bit key, which are attached as the last part of RFDS key.

Consider a mobile phone or washing machine, it can only perform the preprogrammed version of operations, and can never predict from its experience or predefined results. Once an antenna senses the passive tag, the server locates the objects and reminds the officials with message or voice through the interactive platform.

Also, the server records the positions of inmates and inmates' behaviors. Physical and behavioral patterns and movement locations are traced and used for activating the corresponding alarms as needed. This smart or intelligent approach provides a way to satisfy the security and health tracking tools to become both secure and intelligent.

II. OVERVIEW OF THE KEY FORMATION TECHNIQUES

The encryption process is divided into two categories as symmetric and asymmetric encryption. Symmetric keys ensure the healthy transfer between sender and receiver with same key for encryption and decryption. Asymmetric keys use separate or public keys in encryption and decryption process.

The computational time of key generation in authentication techniques is classified as encryption or decryption time, key generation time, and key exchange time between the sender and receiver.

The main focus is given to find the finest protection algorithm, which afford the high defence and also take a smaller amount time for a key generation, encryption, and decryption of data. The time is considered by converting a data file into ciphertext.

Any key production time depends on the size of key length, which is different for symmetric and asymmetric cryptography (Huet al., 2018). Encryption ciphertext exchange time is depending on the communication channel between sender and receiver.

DES algorithm shows it is not quicker for software purpose, but the efficiency of DES is good on hardware. The decryption algorithm differs significantly from the encryption algorithm. Even though, very parallel steps are used in encryption and decryption, their functionalities are not same and the order in which the steps are raised is dissimilar.

In decryption process, each round goes through four steps as follows: Inverse shift rows, Inverse substitute bytes, add round key and inverse mix columns. Various key generation techniques compared are as shown in Figure 2.1.

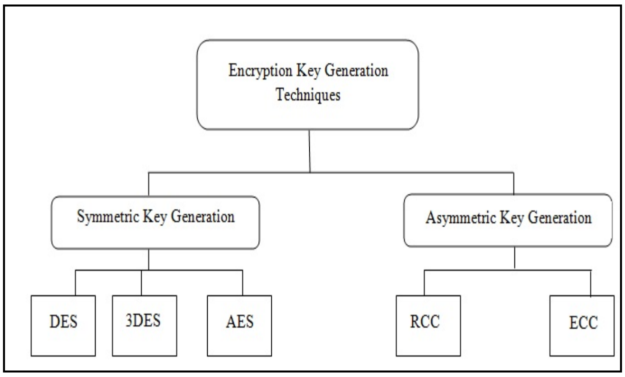

Encryption Key Generation Techniques
Symmetric Key Generation
Asymmetric Key Generation
DES
3DES
AES
RCC
ECC

Figure 2.1: Taxonomy of Key Generation Techniques

The evaluation or the performance of symmetric and asymmetric key generation techniques are analyzed by means of different factors such as time taken for encryption process, decryption time, and key generation time. The AES and DES algorithms are implemented using the Java platform to compare the performance of key generation. Various data size files include in the experiment in our experiments such as 16 KB, 32 KB, 126 KB, 200 KB, 246 KB, and 280 KB and random file size in kilobytes.

AES algorithm employs in small strategies for encrypting a communication to send through a network (Renet al., 2016). Encryption time increases by the size of data file increases. The performance of encryption process increase depends on file size and do not depend on the data type of a file. The efficiency of DES, 3DES is lesser when compared to AES. The AES encryption process has 10, 12, and 14 rounds for encryption based on the data size (Zhuanget al., 2014).

III. PREDICTION PARAMETERS FOR ENHANCED DECISION MAKING IN SEARCH PROCESS

Sensors and RFID readers continuously monitor the inmate's activities and the data are used to generate the 16 bit RFAS key. The individual preferences are found, and analysis is done with pattern-generation algorithms.

The sensor values observed are classified into Critical Actions, Room or body temperature, Health sensor values, and Movement history are given as the input to generate the appropriate behavioral pattern.

Based on this pattern, a flag value will be represented between 0 and 9 and stored in the prediction variable "P.". To enhance the decision making for best search, this last 8 bits are used in alpha-beta pruning algorithm.

C, T, M, and P variables indicate critical actions to be taken, temperature, and physical movement and prediction values.

Passive tags with the properties are used in this experiment analysis. When an inmate leaves a particular area, the RFID reader beside the door scans all the tags attached to the wristband, and makes corresponding alarms. Various intelligent sensors and readers are placed in each entrance and common areas. The inmates are not treated properly, and they face either mental or physical discrimination at times.

Not only the inmates but for the employees also it is difficult to identify the real problems of the inmates (Rostampouret al., 2015).

Agent technology has been considered as an important approach for developing industrial or official secured systems. It offers a more appropriate way to the development of complex computational systems in open and dynamic environments.

Particularly in combination with radio-frequency identification (RFID), intelligent agents have been recognized as a promising paradigm for the latest security measures (Denget al., 2018). The hypothesis combines the RFID passive tags and smart sensors to generate a cost-effective and error-free for authentication as well as monitors the specific environment with a predictive nature.

A combination of these two technologies must be done to obtain the health and behavioral issues of human being in a different environment. The smart agents must be able to find or predict future solutions according to the dynamically changing health and behavioral issues. They can’t predict the nature or activities of inmates instead they are just storing the gathered information.

The role of proposes technology can continuously monitor the inmates and a smart agent helps to predict the future for the various environments with a highly secure authentication method.

IV. RESEARCH CONTRIBUTIONS & RESULTS

A group of jail inmates and the structural information are taken for this proposed RFAS key generation, Authentication, and Search enhancement. All the information in the papers regarding the crime, arrests, personal information, and health track records are collected stored in order. Government- and court-related documents kept separate and secured.

According to the crime and types of punishment individual sets of rules are made to make entry restrictions in various parts of the jail. Duration of custody of each inmate stored to give correct intimations to the officials and authorized users. To manage the collected information, first step taken is organized the inmate’s particulars in an official order.

Second step is the exact interpretation of rules and living aids beneficial to the inmates and employees based on jail mission, vision, and government rules. Third step is done to handle unexpected emergencies or the system failure alternatives. Fourth step collected the decisions and percept history of inmates.

Final step is done to incorporate the predicted decisions with required official permission with a small time span.The sources of data are found by selecting the appropriate and minimum RFID readers and sensors to accomplish the entire research purpose.

Three small jail population samples are taken into consideration and the appropriate sampling procedures are selected. An observation checklist is maintained for each inmate (Kamran Ahsan et al., 2010).

The exposure assessment considered different factors such as the entry exit points in the jail including the visitor and administrator centre. The prison accommodation and service blocks are categorized separately. Entertainment, reading, and smoking are considered with more secure decision parameters to avoid unnecessary fights and collisions between the inmates.

The surrounded fence is also under the RFID and sensor control.When analyzing the behavioral patterns, there is a wide range of differences between individuals even though the sample represents the entire group. People are less homogenous than any other factor.

The Jailor would follow these steps to create a stratified sample of his 400 inmates. The population is 4000 inmates. The desired sample size is 10% or 400 inmates. The factor considered is the inmate’s daily activities or physical level.

There are four subgroups: criminals, petty cases, self-defensive, and mentally retarded. Classified the 400 inmates into different subgroups and found 35% are criminals, 30% are petty cases, 15% are self-defensive and 20% are with mental problems.

The jailor wants 400 inmates in the sample. So, 35% are criminals, 30% are petty cases, 15% are self-defensive, and 20% are with mental problems. This is a proportionally stratified sample. The jail now has a sample of 400 (140+120+60+80) inmates, which is representative of the 4000 inmates and which reflects proportionally each behavioral level.

A major group is taken into consideration and subgroups are formed. Stratified sampling methods are used in this experiment. Out of 4000 jail inmates, a randomly selected 400 inmates are taken into consideration and divided into different categories. Each category is considered as a stratum.

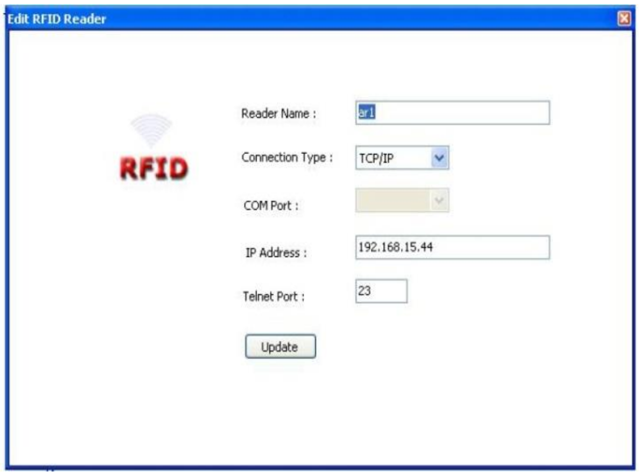
These subgroups can generalize the properties of a large group and can formulate standard methods. Equal size sample subgroups are formed by randomly selecting the same number of subjects from each population subgroup.

Proportional subgroups are formed by selecting behaviors and usual movements so that the subgroup percentages in the population are reflected in the new methodology. The RFAS is based on the sensor and tag values and passed as the ciphertext to the algorithm so it reduces the time complexity in calculating the repetitions of transformations. This study adopted several modes for assessing the inmate’s attitudes on the smart RFID systems. Many conversations conducted with the inmates and semi-structured interviews conducted with the employees.

The modes for acquiring insights on inmate’s attitudes on the use of the RFID and intelligent agents were also the modes used to assess the inmate’s state of knowledge.

The RFID server panel used in this application allows the users to set the different readers with its properties. The user interface makes the server information settings easy and convenient.

Any authorized persons can customize the server setting as and when required with proper authentication. Server panel allows giving customized names to the readers and setting the different connection types. IP address, telnet port, and COM port are set by the administrative users as shown in Figure 4.1.



Reader Name : sr1

Connection Type : TCP/IP

COM Port :

IP Address : 192.168.15.44

Telnet Port : 23

Figure 4.1: Selections of Readers and Server with RFID Server Panel

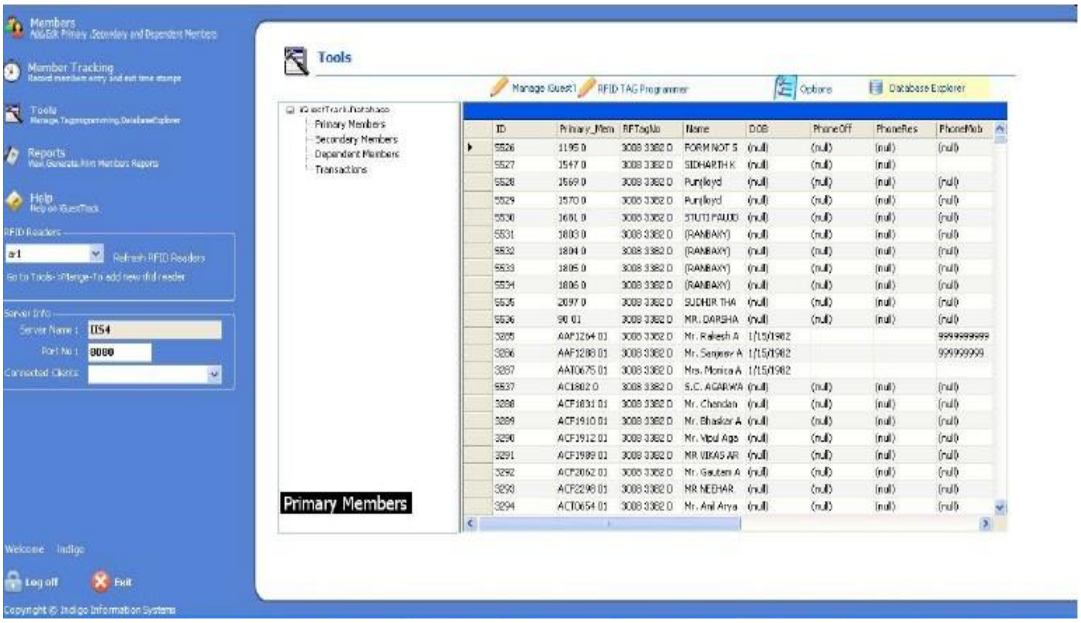
Server panel updates are reflected in all the properties and the changes made are taken into considerations for the RFAS key generation process. This interface maintains the integrity, security, and error handling in an efficient way. Maximum limits on adding the number of readers and IP addresses kept through this interface as shown in Figure 3.5. A popup window enables the different users on adding the same. Different parameters such as reader ID, antennas attached to each reader, distance to be read, and location properties are set to help the interface to make the reading accurate.

As the passive tags used do not have the power supply and has to identify the readability of each antenna. If there are some collision issues or tags are read which are not meant to be in a particular location can be avoided through this interface (Mejjaouli S et al, 2014).

The system keeps track of member's entry and exit and display visitors or inmates who are in the premises, and the amount of time spent in the premises. Various reports such as entry time, the frequency of visits, at premises, contact information, and family member's information can all be stored and displayed in the system.

The administrative panel sets the rights to different users inside the jail environment. Different types of users such as jail officials with different rights from the higher level to lower level, office staffs, doctors, inmates with different levels of criminal records, which leads to different access rights, inmates with mental or physical challenges and visitors.

Administrator panels set all these rights. All entries and exits made in the proximity of readers are designed by this panel. Accuracy and privacy in terms of hardware devices are controlled over this panel. Inmate's wristband with tag information and sensors are tuned in this panel (Ajinkya C et al., 2016). Different RFID and intelligent sensor modules are incorporated in this administrator panel. The user interface provided for the independent admin right users are as shown in the interface screen as in Figures 4.2.



RFID Readers

sr1 Refresh RFID Readers

Go to Tools->Manage->To add new rfid reader

Server Info

Server Name : IIS4

Port No : 8080

Connected Clients :

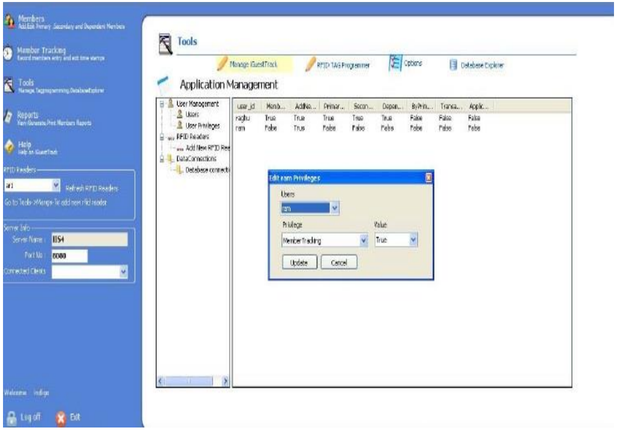
Welcome Indigo

ID	Primary_Mem	RFTagNo	Name	DOB	PhoneOff	PhoneRes	PhoneMob
5526	1195 0	3008 3382 D	FORM NOT S	(null)	(null)	(null)	(null)
5527	1547 0	3008 3382 D	SIDHARTH K	(null)	(null)	(null)	
5528	1569 0	3008 3382 D	Punjlloyd	(null)	(null)	(null)	(null)
5529	1570 0	3008 3382 D	Punjlloyd	(null)	(null)	(null)	(null)
5530	1681 0	3008 3382 D	STUTI PAUJO	(null)	(null)	(null)	(null)
5531	1803 0	3008 3382 D	(RANBAXY)	(null)	(null)	(null)	(null)
5532	1804 0	3008 3382 D	(RANBAXY)	(null)	(null)	(null)	(null)
5533	1805 0	3008 3382 D	(RANBAXY)	(null)	(null)	(null)	(null)
5534	1806 0	3008 3382 D	(RANBAXY)	(null)	(null)	(null)	(null)
5535	2097 0	3008 3382 D	SUDHIR THA	(null)	(null)	(null)	(null)
5536	90 01	3008 3382 D	MR. DARSHA	(null)	(null)	(null)	(null)
3285	AAF1264 01	3008 3382 D	Mr. Rakesh A	1/15/1982			9999999999
3286	AAF1288 01	3008 3382 D	Mr. Sanjeev A	1/15/1982			99999999
3287	AAT0675 01	3008 3382 D	Mrs. Monica A	1/15/1982			
5537	AC1802 0	3008 3382 D	S.C. AGARWA	(null)	(null)	(null)	(null)
3288	ACF1831 01	3008 3382 D	Mr. Chandan	(null)	(null)	(null)	(null)
3289	ACF1910 01	3008 3382 D	Mr. Bhaskar A	(null)	(null)	(null)	(null)
3290	ACF1912 01	3008 3382 D	Mr. Vipul Aga	(null)	(null)	(null)	(null)
3291	ACF1989 01	3008 3382 D	MR VIKAS AR	(null)	(null)	(null)	(null)
3292	ACF2062 01	3008 3382 D	Mr. Gautam A	(null)	(null)	(null)	(null)
3293	ACF2298 01	3008 3382 D	MR NEEHAR	(null)	(null)	(null)	(null)
3294	ACT0654 01	3008 3382 D	Mr. Anil Arya	(null)	(null)	(null)	(null)

Figure 4.2: The Monitoring Mode of RFID Administrator Panel

Member's panel is the user interface with restricted privileges with some administrative rights. Certain members are given the partial access right to the reader and sensor settings to be used in case of emergency situations. Member's panel allows making some readers active or inactive stage so that entry or exit can be controlled. This type of privileges through member's panel gives more accuracy and makes less effort by avoiding single administrator dependencies. The members monitoring mode makes the interface more efficient and useful as it stores the inmate's entry-exit as well as the privileges they used and stores the same. This percept history is used in RFDS key generation along with sensor predictions.

Inmates can be tracked and identified by this interface. The usual choices of the inmate's location partially describe the behavior such as the smoke room, libraries, and outdoors. By these precepts, the individual's preferences are set for one month and if any unusual entry or exit comes inside the jail it is intimated to the officials immediately. Member's panel also provide an editing mode option, which gives the emergency rights to act on readers and sensors. Inside the jail, some restrictions are insisted such as the entry-exit, and close proximity between inmates (Mejjaouli S et al., 2014). Any of these are violated immediate actions are to be taken by the administrators as well as some members who are given the rights. This interface provides the options as shown in Figure 4.3.



user_id	Memb...	AddNe...	Primar...	Secon...	Depen...	ByPrin...	Transa...	Applic...
raghu	True	True	True	True	True	False	False	False
ram	False	True	False	False	False	False	False	False

Figure 4.3: Editing Mode of RFID Members Panel

Editing mode is provided a minimum of two users. Each of them has to enter the user id password in a given order as the first-person username and second persons password and vice versa to ensure no misuse done in changing the settings of intelligent RFID system implemented (Takagi et al., 2015).Reader panel divides the users as primary, secondary, and dependants to give different kinds of access rights and privileges. Primary members are restricted to five where two are jail officials, one doctor, one ministry member, and one psychologist. Secondary users are a group of seven members as subordinate officers under primary members, technical staffs, and software experts.

The experimental with different data size and in term of encryption considered the key generation, encryption, and decryption time. Experimental results showed that RFAS key encryption and decryption time are better compared to AES and DES symmetric key generation. Key agreement and key distribution are the main issues in DES algorithm that takes more time. The comparative results with prefixed data size are as shown in Table 4.1.

Table 4.1: RFAS Key Generation Time for Prefixed Data size

Encryption Key (Symmetric)	Data Size in Kilobytes	Encryption Time in Seconds	Decryption Time in Seconds
DES Key Generation and Processing	16	0.21	0.34
	32	0.32	0.62
	126	0.87	0.69
	246	1.25	1.11
	280	1.78	1.54
AES Key Generation and Processing	16	0.16	0.14
	32	0.18	0.15
	126	0.44	0.43
	246	0.99	0.95
	280	1.09	1.02
RFAS Key Generation and Processing	16	0.12	0.11
	32	0.18	0.14
	126	0.35	0.35
	246	0.87	0.86
	280	1.01	1.01

The following example is a proportionally stratified study of jail environment. The RFAS key reduces the number of key formation steps to 5 for ciphertext generation in all three variants with AES 128-bits, 196-bits, 256-bits, and DES algorithms (Gaurav Beradet al., 2016). The minimal steps involved in the fuzzy blended key generation in any bit length AES algorithm are7 and in DES algorithm it is 8 (Sonali Nimbhorkaret al., 2013). Key length dynamically changes in AES and DES algorithms based on the inputs; whereas, RFAS key follows a standard key length to 16-bits. The encryption time taken for varying input data is as shown in Table 4.2.

Table 4.2: RFAS Key Generation Time for Random Data Size

Input Data Size (Kilobytes)	Time (Seconds)
20000	0.25
40000	0.5
80000	1
160000	2
320000	4
640000	8

The major constraints set for analyzing the prison are as stated in the section. The total capacity of the jail and the number of inmates are intimated before reader and sensor settings. The estimated average length of stay of inmates is collected and alarms set for privileges. The number of admissions in case of emergencies gave provisions to get added to the smart environment. While considering human nature, the need to utilize and apply the latest and secure methods or protocols to help to improve inmate’s lives is important and requires accurate, near-real-time data gaining, and assessment. At the same time, the inmate’s data need to be private and secure. The best way for this is the combination of intelligent agents and RFID. This technology can use wireless networks for fast data collection and transmission while maintaining the privacy issue. The mental and health records from the medical team and inmates are recorded. Categorizing the inmates by age, crime, the period of stay, and language is done. The operational areas of inmates are divided. Non-functional areas in the jail are separated from another area. Rights for officials inside the different blocks are set on devices. Minimum facility available for inmates and officials is described. The graphical representation time taken for encryption is as shown in Figure 4.4.

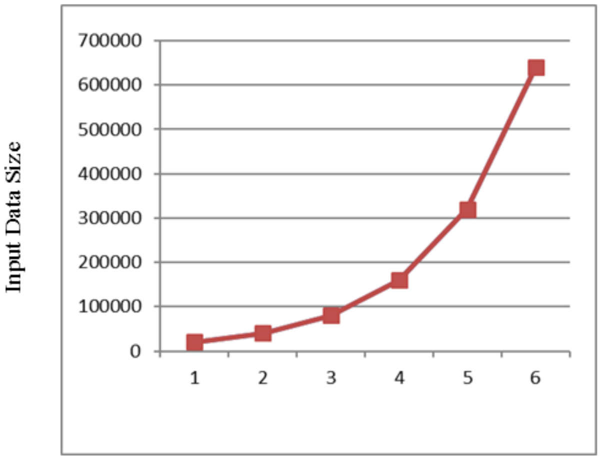


Figure 4.4: RFAS Key Generation Time for Different Data Size

Inmates are monitored by a centralized smart environment. The information is stored in the tag and in a smart server. Registering pertinent information regarding the inmates, along with the guest preferences, helps to record inmate's behavioral patterns, health, and expected levels of freedom. Intelligent agent's help to suggest or predict the mental and physical changes of the inmates and smart alarms can be generated according to the age, decease, and activities. Results are considered with various authentication and decision-making search algorithms. The enhanced technique considers three factors compared to the other authentication algorithms. Any algorithm is designed in such a way that the time taken for encryption or decryption must be similar and provides a faster result.

The RFAS key once generated is used at both the end of encryption and decryption. AES key is based on the number of repetitions of transformations. The confidentiality must be kept in all aspects of the information-gathering process. During and after the research procedure, data must be filed with security features both in systems and physically. All sources of data that were indicative of the identity of inmates in the action research must be destroyed after completion of the project. The other factors are education level of inmates, sentenced/not, entertainment factors, and social activities.

V. CONCLUSION

This paper discusses the key generation with RFID and sensors. The RFAS key is efficient and secure in terms of time for key generation, steps involved in the procedure and providing a standard key length of 16-bit. The maximum number of steps required to generate to RFAS key reduced to five where other major encryption it is higher. Key length dynamically changes in AES and DES algorithms based on the input data block size. The time taken for key generation also decreases, which helps in enhancing the authentication and search process.

REFERENCES

1. Abdolmaleki, B, Baghery, KAkhbari, B, 2014, 'Attacks and Improvements on Two New-Found RFID Authentication Protocols', 7th *International IEEE Symposium on Telecommunications,* pp. 895–900.
2. Abdulhadi AE, Abhari R, 2012, 'Design and Experimental Evaluation of Miniaturized Monopole UHF RFID Tag Antennas', IEEE *Antennas Wireless Propagation Letter,* vol. 11, pp. 248–51.
3. AHN, H.S, Yoon, E.J, Bu, K.D, 2013, 'Improved U-Healthcare Service Authentication Protocol based on RFID Technology', *Journal of Institutional Electronics Information Engineering,* vol.50, pp.107–115.
4. Alallayah, Khaled M, 2012, 'Applying Neural Networks for Simplified Data Encryption Standard (SDES) Cipher System Cryptanalysis', *Arab Journal of Information Technology,* vol. 9, pp.163-169.
5. AL-Hamami, A, AL-Hamamim M, Hashem S, 2011, 'A Proposed Modified Data Encryption Standard Algorithm By Using Fusing Data Technique', *World of Computer Science and Information Technology Journal,* vol. 1, pp. 88–91,
6. Amin, E M, Saha, J K Karmakar, N C, 2014, 'Smart Sensing Materials for Low-Cost Chipless RFID Sensors', *IEEE Journal of Sensors and Actuators,* vol. 14, pp. 2198–2207.
7. Avoine, G, 2015, 'Cryptography in Radio Frequency Identification and Fair Exchange Protocols', *Info Science Publications,* vol. 7, pp. 267–274.
8. Al-Turjman FM, Al-Fagih AE, Hassanein HS, 2012, 'A Novel Cost-Effective Architecture and Deployment Strategy for Integrated RFID and WSN Systems', *International Conference on Computing Networking and Communication,* pp. 835–839.
9. G Avoine, E Dysli, P. Oechslin, 2005, 'Reducing Time Complexity in RFID Systems', Proceedings of the 12th *International Conference on Selected Areas in Cryptography,* pp. 291–306.
10. Bhattacharjee, Roy, S. Ghosh, P. Misra, S,Obaidat, S, 2012, 'Wireless Sensor Network-based Fire Detection, Alarming, Monitoring and Prevention System for Bord-And-Pillar Coal Mines', *Journal of Systems and Software,* vol. 85, pp. 571–581.
11. Y. Bayram, Y. Zhou, B. S. Shim, S. Xu, J. Zhu, N. A. Kotov, and J. L. Volakis, 2010, 'E-Textile Conductors and Polymer Composites for Conformal Lightweight Antennas', *IEEE Transactions Antennas Propagation,* vol. 58, pp.2732–2736.
12. M. Burmester, T Van Le, B De Medeiros, 2006, 'Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols', *IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks,* pp. 401-410.
13. T. Björninen, M. Lauri, K. Koski, L. Ukkonen, A. Z. Elsherbeni, R. Ritala, L. Sydänheimo, 2011, 'Wireless Measurement of Wake-Up Power and Impedance of UHF RFID IC', *Proceeding of AMTA Symposium,* pp. 63–68.