ISSN 0975-2366
https://doi.org/10.31838/ijpr/2018.10.04.018

Research Article

Integration of RFID wireless tags and intelligence to enhance authentication in smart environments

V. VISHU[1*], R. MANIMEGALAI, SABULAL ANANDAN,[2] KOTTAKKATTUTHARAYIL[3]
Research and Development Centre, Bharathiar University, Coimbatore, India. Email:vishusabulal@gmail.com
Research and Development Centre, Bharathiar University, Coimbatore, India. E-mail:mmegalai@yahoo.com
Research and Development Centre, Bharathiar University, Coimbatore, India.E-mail:sabulaal@gmail.com
Received: 18.07.18, Revised: 6.08.18, Accepted: 28.09.18

ABSTRACT
The paper presents a smart encryption method by combining RFID passive tag values and intelligent sensor values. The main challenges are metallic environment reflection, security, privacy and cost. The method evaluates the interaction between RFID and medical/security sensors, and identifies the factors which had a significant influence on the level of inmate's mental and physical challenges. The proposal is to apply an enhanced smart key in encryption on independent living or to assist them for a good life.

Key words : Intelligence, Sensors, Radio Frequency Identification Readers and Tags, Smart AES Algorithm

INTRODUCTION

This paper proposes an outline of autonomous control agents for distributed jail management systems. Intelligent Agents and Radio Frequency Identification (RFID) are the groundwork of the concept presented here. The method adds a new SMART Key into the Advanced Encryption Algorithm. The procedure is as given below

- o ADD ROUND KEY
- Substitute Rows
- Shift Rows
- Mix Columns

o ADD ROUND KEY

The Round Key will be supplied as the CYPHER Text of 16 bits in normal AES Algorithms. The new methodology creates CYPHERTEXT as two 8-bit Values where first 8-bit value will be indicating the RFID Tag value and the second half will be the sensor values as in figure 1.

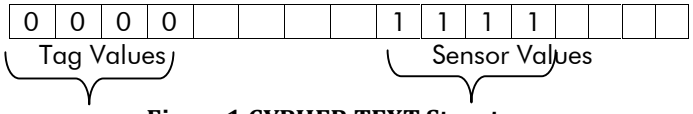

Figure1.CYPHER TEXT Structure

Here the new ROUND key applied to the AES Algorithm will be a 16 bit Key which will enhance the encryption algorithm with less time, less number of transitions and minimum use of Memory. Consider a mobile phone or washing machine, it can only perform the pre programmed version of operations, and can never learn a new thing from its experience or pre-defined results. This smart or intelligent system provides a way to satisfy the security and health tracking systems to become both secure and intelligent. Agent technology been considered as an important approach for developing industrial or official secured systems. It offers a new and 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 latest security measures. In the commonly increasing crime face, a new method or technology for identifying the cause of increase in crime, the mental state and also the health issues they are facing must be there to reduce the crimes or to identify the real problems. So the new system must be designed in such a way that it can be easily adapted to the changes, environment and users. It must be able to cop up the unexpected errors or changes in order to minimize possible errors on the environment. This technology provides a way to satisfy all these requirements because it enables security systems to become both secure and intelligent.

OVERVIEW

Intelligence and RFID

The data collected using the RFID sensors must be transformed to knowledge or information for the agents. This agent must be able to work on these data and new dynamic data to produce best results. A set of assessment or predictions must make in the absence of human beings. In this proposal a jail environment is considered and the data include medical and physical movements or changes.

RFID Components

Radio-frequency identification (RFID) technology uses radio frequency signals to acquire data remotely from tags within read range. The data is then used for a variety of purposes such as opening doors and gates, paying tolls or tracking equipment and materials or human beings. Radio-frequency

identification (RFID) uses radio waves for the identification of humans or items. The RFID system consists of a reader and a transponder component called as a tag which is associated with various objects. Tags are classified into two types Passive tags and Active Tags. The RFID systems use the method of energy and data transfer using transmission of radio signals Identification of objects is performed on the basis of a unique identifier, which is stored on the tag. The tag itself consists of at least an integrated circuit and an antenna. RFID tags are more resistant to various environmental influences like water, dust, oil, paint, etc. It is possible to read up to hundreds of RFID tags simultaneously – even through objects. **Tag-**RFID tags are device that contain identification and other information that can be communicated to a reader from a distance. An **RFID tag** is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked. "RFID" stands for Radio Frequency Identification. The tag's antenna picks up signals from an RFID reader and then returns the signal, usually with some additional data (like a unique serial number or other customized information).RFID tags can be very small - the size of a large rice grain

Reader - A reader may be referred to as an "interrogator" because it asks (or interrogates) tags for their ID information and any other data they may contain.

Antenna(s) - The antenna broadcasts the RF signals generated inside the reader's transmitter into the immediate environment. The antenna also receives responses from tags within range.

RFID Users

The users can be categorized into two types like Administrators and Members the first user account to be created is of type Admin. Members can be classified as the primary secondary and dependants for the inmate's A new protocol which will be avoiding the anti collision problems of RFID passive or active tags in metallic environment and at the same time include an intelligent agent which can predict the future behavior of the inmates

Hypothesis

The methodology which is going to be installed in a metallic environment must solve the multiple tag identification within a short range and collision issues. At the same time an intelligent agent must identify the signals from various sensors like medical sensors, environmental sensors and RFID sensors, and apply the pattern recognition methods to identify the behavioral and health patterns of objects and humans to generate the health and warning alarms. The method must be useful for different age people to continuously monitor their body level without a physical presence.

Results

While considering the human nature, the need to utilize and apply the latest and secure methods or methods 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 needs to be private and secure. The best way for this is Combination of Intelligent agents and RFID. This technology can use wireless networks for fast data collection and transmission while maintaining the privacy issue. Inmates will be monitored by a centralized smart environment. The Information will be stored in 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 agents will 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

OBJECTIVES

The new method will help the agent to accomplish the given tasks automatically based on the types of users. The agent describes a software unit. Here the Agent not always works like a software unit, i.e.; it can be a sensor or an object. In this proposal it will be appropriate to use the cognitive agents. Cognitive agents give an exact environmental model based on the set of beliefs, intensions and desires. It will never be bothered about the behavior. The set of preferences and the goals of the environment can be acquired by this environment. The various actions of the agents will be based on the constantly changing environments and those plans will be stored in the computer memory. In this face RFID and other sensors will have its role. So based on all these factors and the current state the agent will predict the future activities of the inmates. Thus the agent will generate the corresponding alarms. A single agent will not be sufficient for the method generation as it will not satisfy the critical problems.

Types of RFID Tags

Passive: Passive RFID tags are designed to be small and low cost. A passive tag only contains an antenna and circuitry that stores data, but does not include an internal power source. Energy required for sending data back to the reader is detracted from the electro-magnetic energy field generated by the reader while trying to read the tag information.

Active: These RFID tags use their own internal battery to send data. Their battery allows them to transmit data up to several hundred meters. Active tags are incessantly or cyclically transmit signals and data, regardless of whether the tag is in the field of a reader or not. In this case the tag acts as a beacon. Depending on the configuration of the tag, it may also have a processor, read-only memory (ROM), which holds the firmware, or memory to store user-defined data. Admittedly, such additional components make active tags also the most

expensive ones.

RESEARCH CONTRIBUTIONS

The hypothesis will combine the new technologies RFID passive tags and Smart sensors to generate a cost effective and error free system which will monitor any 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 an extra ordinary environment. The smart agents must be able to find or predict the future solutions according to the dynamically changing health and behavioral issues. The specific aims of this method can be sown in the Figure 2.

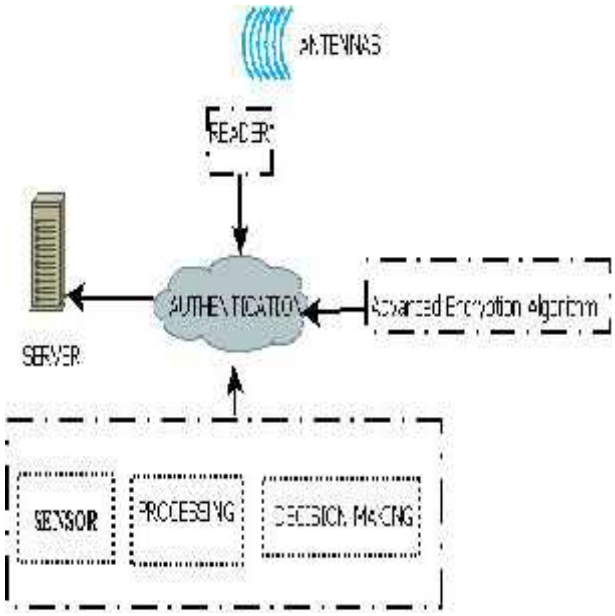

Figure 2. An Adaptive Authentication Smart Key

BACKGROUND AND SIGNIFICANCE

The main significance of this proposal is from the issue that occurs for the unusual human beings. In any jail inmates are not treated properly they are facing either mental or physical discrimination at times. Not only the inmates but it will also be a headache for the employees to identify the real problems of the inmates. Cameras and doctors of course play a great role to solve these issues. But they can't predict the nature or activities of inmates instead they are just storing the gathered information. Here comes the role of new method which can continuously monitor the inmates and a smart agent will help to predict the future for the various environments.

Literature Review

As per the Intelligent agents research articles an intelligent agent is software that assists people and acts on their behalf. Intelligent agents work by allowing people to delegate work that they could have done, to the agent software. Agents can, just as assistants can, automate repetitive tasks, remember things you forgot, intelligently summarize complex data, learn from you, and even make recommendations to you. In the recent research trends says that all agents are also goal-driven. Agents have a purpose, and act in accordance with that purpose. There are several ways of making goals known to an agent, however: A rudimentary agent could be driven by a script, which pre-defines its actions. The script would then define the agent's goals. An agent could also be a program, as long as the program is driven by goals, and shares the other characteristics of agents. An agent could also be driven by rules, which is a more general way of defining the agent's goals. There are even more sophisticated ways of embedding agent goals, such as "planning" methodologies, and in some cases, the agent may even have the flexibility to change its own goals over time. All agents are also reactive. That is, an agent senses changes in its environment and responds in a timely fashion to these changes. This characteristic of agents is also at the core of delegation and automation. Just as you tell your assistant, "When A happens, do B" an agent is always waiting for A to happen! Finally, in order to carry out the wishes of the user, all agents continue to run, even when the user is gone. This implies than an agent may run on a server, but in fact some agents run on user systems. As per the recent research trends in RFID and Intelligent agents considering privacy, limited privacy protection is a major concern for individuals by the article by Zappone. The cost of tags and readers is the next issue. Current projections are to have tags that cost about 5 US cents each in order to facilitate wider adoption of RFID for tagging individual items. In the M. Burmester, T. van Le, and B. de Medeiros. Provably secure ubiquitous systems: Universally composable RFID authentication methods. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2006,

Baltimore, Maryland, USA, August-September 2006. IEEE. [4] T. Dimitriou. A lightweight RFID method to protect against traceability and cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005, Athens, Greece, September 2005. IEEE It appears that the target of 5 US cents per tag is arbitrary, as the attempts to find an economic justification for this target have failed and so costs may not be as a big a drawback on wider adoption as some might be claiming. In the G. Avoine. Cryptography in Radio Frequency Identification and Fair Exchange Methods. PhD thesis, EPFL, Lausanne, Switzerland, December 2005, RFID systems have become synonymous with "insecure" systems, a situation that must be thoroughly addressed before it severely limits widespread deployment of RFID systems. Research in security and privacy is arguably the most active area in RFID research at the moment. This view is backed by an inspection of the publication dates of papers in G. Avoine, E. Dysli, and P. Oechslin. Reducing time complexity in RFID systems. In B. Preneel and S. Tavares, editors, Selected Areas in Cryptography – SAC 2005, volume 3897 of Lecture Notes in Computer Science, which shows the number of RFID security-related publications growing annually from 1 in 2002 to 65 in 2006 (Avione 2007). Juels surveys the current research in this area, the components receiving the most attention are the tags; he categorizes them as basic RFID tags, which are passive, chip less tags, and symmetric RFID tags, which are primarily active, chip-based tags. RFID system designs where tags promiscuously surrender their identity when queried by any interrogator operating at the appropriate frequency cannot be tolerated in a secure environment. A multi-step authentication process is required in order to create a secure channel of communication between the tag and the interrogator. T. Dimitriou. A lightweight RFID method to protect against traceability and cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks – Secure Comm 2005, Athens, Greece, September 2005. IEEEs have gone further and proposed custom RFID cryptographic processors for this task. Low cost tags are for the most part passive; they do not have an on-board power source, they derive their power from the signal sent by the interrogating reader. As a result they generally are, smaller in size, chip-less, easier to manufacture and to apply onto products and require no in-field maintenance. The power characteristics of the tags influence the frequency and potential applications of an RFID system, as the table below shows. (As per the Research trends article)

In addition to passive and active RFID tags, there are also two hybrid forms: *semi-passive* and *semi-active* tags. Just like active tags, both types include an internal battery. However, semi-passive tags do not use their internal battery to send data back to the reader. Although it is still using the "backscattering" mechanism, the purpose of the battery is to keep the tag powered even when it is not being read. This allows the tag to continuously monitor its environment and process data. Energy required for data transmission is still induced by the reader as it attempts to read the tag. On the other hand, semi-active tags use the battery for data transmission, but they do not remain active all the time. Instead, they have to be activated by a low frequency signal coming from the reader. Then, they are switching back to a sleeping-mode when not used. Compared to active tags, lower costs and longer battery life are motives for using semi-passive or semi-active tags

Table 1. Frequency Range of RID Passive Tags

Frequency	Distance
Low frequency LF	125-134 k HZ cm
High Frequency HF	13.56 MHz 1m
Ultra High Frequency	860 - 930MHz 3m

Methodology

Methods

The primary goal of this intelligent system is making the accused living more efficient and convenient. This system can provide both location tracing and health alarms. Passive RFID tag locate the inmates physical and health related activities and can also identify the presence of any electronic device. When an inmate leaves a particular area, the RFID reader beside the door will scan all the tags attached to his wristband, and makes alarm if he /she is not supposed to leave intelligent sensors and readers will be placed in each entrance and common areas. Once an antenna senses the passive tag, then server will locate objects and remind the employees with message or voice through the interactive platform. Also, the server records the positions of inmates and inmates' behaviors.

Study Sample

It is a fact that the reasoning is an important part of any scientific analysis. For example reasoning can be found from individual inmate observations to general strategies. If the observations made from different set of individuals and groups are gathered and analyzed properly, standard conclusions or decisions can be made. Here in this proposal the population to be considered is too large or scattered in different parts of the world. So it will be appropriate to take any three different jails and make some common decisions or predictions to make the conclusions based on the general characteristics of inmates. Stratified sampling and randomization can be used in this proposal for sampling. This is the process of arbitrarily selecting population members for a given

sample, or randomly assigning topics to one of several experimental groups, or randomly assigning experimental treatments to groups. it is selecting topics for a sample in such a way that every member of the population has an equal chance at being selected

The Sampling Method, Sampling size and the Target Population

Stratified sampling permits the researcher to identify sub-groups within a population and create a sample which mirrors these sub-groups by randomly choosing subjects from each stratum. Such a sample is more representative of the population across these sub-groups than a simple random sample would be. Subgroups in the sample can either be of equal size or proportional to the population in size. Equal size sample subgroups are formed by randomly selecting the same number of subjects from each population subgroup. Proportional subgroups are formed by selecting subjects so that the subgroup percentages in the population are reflected in the sample. The following example is a proportionally stratified sample.

The Jailor would follow these steps to create a stratified sample of his 400 inmates.

1. The population is 4000 inmates
2. The desired sample size is 10%, or 400 inmates
3. The factor considered will be inmate's daily activities or physical level l. There are four subgroups: criminals, petty cases, self defensive, and mentally retarded
4. Classify the 400 inmates into the subgroups. In this case, 35% are criminals, 30% are petty cases, 15% are self defensive and 20% are with mental problems.
5. 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.
6. 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.

Cost Effectiveness

If the sample size increases the money value and the total time required will increase. The balancing must be done between sample size, money value and time.

Error Free

Whenever implementation happens there will be a huge difference between the actual results and the expected ones. The main aim is to reduce the difference so as to lead to an efficient project. The unexpected causes may delay or affect the working modules. When the target size increases the possibility of errors also increases.

The nature of the population

When analyzing the behavioral patterns there will be a wide range of differences between individuals even though the sample represents the entire group. People are less homogenous than any other factor.

Exposure of Assessment

The Entry Buildings including the Visitor and administration Centre The Prison Accommodation and Services Blocks The Sports/Multifunctional Hall The Prison will be surrounded by a high security wall on all sides.

Results

The efficient management of a jail system is important not only for the day-to-day operation of those running that system, but also to the inmates within the system. A well-organized approach to jail management means officials can perform their jobs more effectively and accurately record inmate activity. An automated jail management system provides the necessary documentation of all inmate activities and automates all functions to ensure due process. The ability of a jail management system to efficiently collect, analyze, and coordinate inmate information plays a vital role in the effectiveness of how a jail is run.

- Privacy must be provided
- Sample data must be evaluated correctly
- Security issues and intelligent agents must be tried frequently
- Time Complexity in seconds for Smart AES algorithm with other Encryption algorithms is given in the figure 2

ANALYSIS STRATEGIES USED

- The total capacity of the jail and the number of inmates should be noticed
- The estimated average length of stay
- The number of admissions of new inmates and the cause
- The mental and health records
- Categorize the inmates by age, crime, period of stay and language
- The operational areas of inmates
- Non-Functional areas in the jail
- Rights inside the different blocks
- Average facility available

Ethics and Human Subjects Issues

This study adopted several modes for assessing the inmate's attitudes on the smart RFID systems. Many conversations conducted by the researcher with the inmates and semi-structured interviews conducted by the researcher 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 by the researcher to assess the inmate's state of knowledge 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 which 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
- Social activities

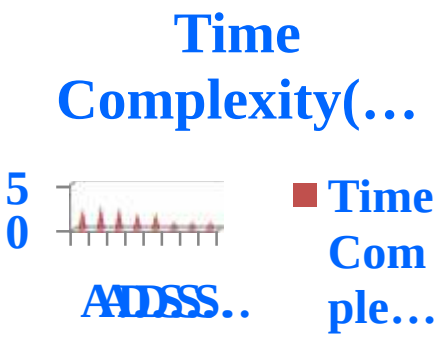

Figure3. Time Complexity Comparison with all Algorithms

Conclusion

The new method will provide an intelligent SMART Key for encryption and future enhancement can be done by analyzing the decision making capability of various sensors to make the algorithm more efficient..

References

1. Y. Ma, L. Zhou, K. Liu, I. Wang, "Iterative phase reconstruction and weighted localization algorithm for indoor RFID-based localization in NLOS environment", *IEEE Sensors J.*, vol. 14, no. 2, pp. 597-611, Feb. 2014.
2. Wang, Y. Ma, Y. Zhao, K. Liu, "A multipath mitigation localization algorithm based on MDS for passive UHF RFID", *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1652-1655, Sep. 2015.
3. Lianbo Ma, KunyuanHua, YunlongZhu, HanningChen Cooperative artificial beecolony algorithmformulti-objective RFID networkplanning. 2009
4. RarickR,SimonD,VillasecaF.E.,VyakaranamB.Biogeography-basedoptimizationand thesolutionofthepower flow problem.In:ProceedingsofIEEEinternational conferenceonsystems,manandcybernetics,2009
5. G. Avoine. Cryptography in Radio Frequency Identification and Fair Exchange Protocols. PhD thesis, EPFL, Lausanne, Switzerland, December 2005. ttp://library.epfl.ch/theses/?nr=3407
6. G. Avoine, E. Dysli, and P. Oechslin. Reducing time complexity in RFID systems. In B. Preneel and S. Tavares, editors, Selected Areas in Cryptography – SAC 2005, volume 3897 of Lecture Notes in Computer Science, pages 291–306, Kingston, Canada, August 2005. Springer-Verlag.
7. T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005, Athens, Greece, September 2005. IEEE
8. M. Burmester, T. van Le, and B. de Medeiros. Provably secure ubiquitous systems: Universally composable RFID authentication protocols. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2006, Baltimore, Maryland, USA, August-September 2006. IEEE.
9. T. Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005, Athens, Greece, September 2005. IEEE
10. A. Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03), Oct. 2003
11. Goudos SK, Siakavara K, Sahalos JN. Novel spiral antenna design using artificial bee colony optimization for UHF RFID applications. IEEE Antennas Wirel Propag Lett 2014;13:528–31.
12. Goudos SK, Siakavara K, Sahalos JN. Synthesis of miniaturized load-ended spiral antennas for UHF passive tags. In: IEEE-APS Topical Conference on Anten-nas and Propagation in Wireless Communications, IEEE APWC 2013. 2013. p. 927–30.
13. Goudos SK, Siakavara K, Sahalos JN. Modified spiral RFID tag antenna optimal design using artificial bee colony optimization. In: 43rd European Microwave Conference, EuMC 20