Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

Reliable Data Transmission and Secured Communications Using Artinian Rings

C.Senthilnathan[1], S.Karunanithi[2]
[1,2]PG & Research Department of Mathematics.,
[1,2]Government Thirumagal Mills College, Gudiyattam,Vellore Dist,Tamilnadu, India.
Affiliated to Thiruvalluvar University, Serkardu, Vellore Dist. Tamilnadu, India.

Abstract:-Several authentication schemes have been proposed for dispersed networks that are cloud-based. Still, the majority of methods are vulnerable to security flaws such replay attacks, privileged insider threats, mutual authentication, and user anonymity. In order to offer security and privacy, this study implements an authenticated environment based on sensors and sensor-tags, utilizing S-USI (single-user sign-in). A strong secure based S-USI mechanism and a well-formed coexistence protocol proof for pervasive cloud services are provided to reinforce the authentication process by using various algebraic structures. The prominence of the suggested techniques is demonstrated to demonstrate the security effectiveness of the suggested S-USI using formal security analysis. The comparison results from the formal verification shows that the suggested S-USI has less computational overhead, making it potentially more appropriate for telecare medical information systems by using artinian rings.

Keywords*:* Artinian rings, cryptography, algebraic structures

I Introduction

Rings are algebraic structures that extend the concept of groups by introducing an additional operation. Rings are essential in coding theory and cryptography as they provide the mathematical framework for constructing error-correcting codes and cryptographic algorithms. In a similar manner, fields are algebraic structures that further extend the concept of rings by introducing the notion of division [4]. Algebraic structures, such as groups, rings, and fields, possess specific properties that are crucial for their applications in coding theory and cryptography. Cyclic groups are groups generated by a single element, and they are extensively used in error-correcting codes and cryptographic algorithms [3]. Polynomial rings provide a powerful tool for constructing error-correcting codes based on algebraic algorithms. Galois fields, also known as finite fields, are fundamental in coding theory and cryptography due to their efficient arithmetic operations. Matrix rings play a crucial role in the construction of linear error-correcting codes and cryptographic algorithms [7, 11].

Understanding the properties and examples of algebraic structures is vital for designing and analyzing coding schemes and cryptographic algorithms [10]. These structures form the mathematical backbone that enables efficient and reliable data transmission and secure communication in coding theory and cryptography [9].

An Artinian ring admits a finite direct sum decomposition as a module over the ring itself ,and this can be written as :

$$P_{i_{P_i}} = P_i m_1 1 \oplus \dots P_i m_1, \mu_1 \oplus \cdots \oplus P_i m_n, 1 \oplus \cdots \oplus P_i m_n, \mu_n \text{ ,(1)}$$

where the $m_{i,j}$are referred as orthogonal idempotents and also primitive with $1 = \sum m_{i,j}$. This decomposition is recognized as a result of the principal decomposition of the module of P_i over itself like a self-loop.We index the $P_i m_{i,j}$with its similarity to $P_i m_{s,l}$if and only if $i = s$,and$j = l$,then we replace$m_i = m_{i,1}$. Hence,

$$P_{i_1} \cong \oplus \mu_i P_i m_i$$

Ingeneralthe element becomes that the base of a module $M_i$which is the summation of the simple non-zero sub-modules [8]. Sub-modules of $M_i$and the fundamental of a module $M_i$are the intersection of all possiblesub-modules of M_i. Then, the module $P_i m_{i,j}$hasa distinctive maximal sub-module of$Rad\ (P_i)m_{i,j} = P_i m_i \cap Rad\ (P_i)$ and a distinctive decayed quotient is defined as$L(P_i m_{i,j}) = P_i m_{i,j}/Rad\ (P_i)m_{i,j}$.

By the fundamental module of $P_i$over itself be decomposed and written like:

$$P_{i_{P_i}} = \oplus\, \mu_i P_i m_i.$$

At the same time, an Artinian ring $P_i$is quasi-Frobenius, if there exists a combination $\tau$with the fundamental module,

$$L(P_i m_i) = U(P_i m_{\tau i}) \tag{2}$$

and

$$L(P_j m_j) = U(P_j m_{\tau j}) \tag{3}$$

Hence the ring is Frobenius, and if$m_{\tau i} = m_{\tau j}$as well.In continuation with this a module $M_i$in excess of a ring $P_i$which is injective and, for respective pair of P_i-modules$T_{i_1} \subset T_{i_2}$and every P_i-linear mapping is defined as, $f: T_{i_1} \rightarrow M_i$ and extend the same to an P_i-linear mapping$f: T_{i_2} \rightarrow M_i$.

II.Preliminaries

Definition 2.1: The Jacobson radical of a ring, indicated by $J_i(R_i)$, is constructed by the elements which annihilate all the simple right R_i modules.

The security of S-USI could be analyzed using the algebraic properties of Artinian rings toensure that it meets required security standards and is resistant to known attacks.

Lemma 2.2: $J_i(R_i)$ is the intersection of all the maximal right ideals of R_i.

Proof : Let I_i indicates the intersection of all the maximal right ideals. Let M_i be a simple right-hand module R_i. If m_k is a component other than M_i, then $Ann(m_k)$ is the right maximal ideal, so it contains I_i where $Ann(m_k)$ denotes the annihilate of the component m_k. Therefore, $m_k I_i = 0$. Since m_k and M_i are arbitrary, it follows that I_i annihilates all the simple modules, so it is contained in $J_i(R_i)$.

Conversely, if L_i is the right ideal of the maximum right, R_i / L_i is simple, therefore $J_i(R_i)$ annihilates it. Therefore, $J_i(R_i) \subset L_i$, and it follows that $J_i(R_i) \subset L_i$. Therefore, $J_i(R_i) = I_i$.

Proposition 2.3 : If R_i is right artinian, then $J_i(R_i)^n = 0$ forlarge n.

Proof : Consider $J_i = J_i(R_i)$. Since R_i is right Artinian, and the chain $J_i \supset {J_i}^2 \supset \ldots$ stabilizes. Suppose ${J_i}^n = {J_i}^{n+1} = \ldots$ and suppose ${J_i}^n \neq 0$. Then choose a right ideal I_i that is minimal subject to the condition that $I_i {J_i}^n \neq 0$. Now choose $a \in I_i$ such that $a {J_i}^n \neq 0$. Since $a{J_i}^n {J_i}^n = a {J_i}^{2n} = a {J_i}^n \neq 0$, the minimality of $I_i$implies that $a{J_i}^n = I_i$. Therefore, there exist an element of $x \in {J_i}^n$in such a way that the approach leads to the conclusion that $ax = a$. Therefore, $a(1 - x) = 0$. But $1 - x$ is an element of ${J_i}^n$, therefore $a = 0$. From this contradiction we deduce that $J_i(R_i)^n = 0$.

Theorem 2.4: If R_i is right artinian, then it is right noetherian.

Proof : Let $J_i = J_i(R_i)$. The Artin-Wedderburn theorem implies that R_i / J_i has a finite length. Since all ${J_i}^k / {J_i}^{k+1}$ factors are right R_i / J_i modules. Therefore, it seems from the consideration of the series $R_i \supset J_i \supset {J_i}^2 \supset \ldots \supset {J_i}^n = 0$ that R_i must also have a finite length as right module R_i. This implies that R_i is right Noetherian.

An authentication scheme like S-USI uses Artinian rings, and this might utilize their algebraicproperties to enhance security [1]. For instance, the ring's properties might be used to construct secure keys, manage cryptographic operations, or ensure the integrity of the authentication process [6].

Proposition 2.5: Let M_i be a module that is either noetherian or artinian. Then M_i is written as a finite direct sum of indecomposable modules.

Proof: The zero modules cannot be decomposed, so suppose that $M_i \neq 0$. If M_i isartinian then it has a sub-module N_i which is minimal subject to the condition that N_i is a direct summand of M_i. If M_i is noetherian, it has a sub-module L_i, which is the maximal subject to this condition, and if N_i is chosen in this way we get $M_i = L_i \oplus N_i$, therefore, N_i is the minimal subject to this condition [2, 5].

It is clear that N_i is not divisible. Now we can write $M_i = N_i \oplus M_{i_1}$. Since M_{i_1} is a quotient of M_i, it inherits the chain condition of M_i, so we can apply the same argument with M_{i_1} instead of M_i to get $M_{i_1} = N_{i_1} \oplus M_{i_2}$ with non-modular N_{i_2}. Continuing in this way, the conditions of the chain ensure thatthe process stops in a limited number of steps, and thus gives the result. Here the question of uniqueness is: if a module is written as an immediate sum of the non-decomposable. The another question arises here is: are the two decompositions essentially the same or differ by each. The primary focuses here is, we need a new way to recognizeand construct the module which is not decomposable [3].

Another important and interesting factor about the ring is :

An R_i ring is local if $R_i/J_i(R_i)$ is a division ring.

Note that this is not the same as saying that R_i has a uniquemaximal two sided ideal.

III Artinian Rings and ideals

Proposition 3.1: For any Artin ring B_i, each prime ideal is maximal

Proof: Assume Q_i as a prime ideal of B_i. Then $P_i = B_i/Q_i$be in an Artinian integral domain. Assume $a \in P_i, a \neq 0$. We now have $(a^r) = (a^{r+1})$ for every r, therefore $a^r = a^{r+1}b$ for every $b \in P_i$. Given that, P_i is an integral domain of B_i and $a \neq 0$, it follows that presently we have got an inclination to decay the value of a^r, since $ab = 1$. Hence, a has degree inverse in P_i, and since p might be a field, such that Q_i might be a maximal ideal.

Proposition 3.2: The finite degree Artinian ring and the nilradical is the finite intersection of Jacobson radical.

Proof: Let the group of all finite intersections $n_1 \cap n_2 \cap \ldots \cap n_r$, where $n_1$is maximal ideals. This set contains a maximal component, let $n_1 \cap n_2 \cap \ldots \cap n_r$, since for any maximal ideal n, we may take the intersections of $n_1$to n_r for every r, since $n = n_j$, hence $n_j$be maximal.

Proposition 3.3: The finite degree Artinian ring and the nilradical $\mathcal{H}_i$ is nilpotent.

Proof:The inclination may shows like $\mathcal{H}_i^r = \mathcal{H}_i^{r+1} = \ldots = \alpha$ and this is possible, for every $j > 0$. Consider $\alpha \neq 0$, and assume $\sum$ denote the group of all ideals pq such that $pq \neq 0$. Then $\sum$ is nonempty,therefore $\alpha \in \sum$. Consider q is a minimal element of $\sum$, after that there exits $a \epsilon q$ that is $a\alpha \neq 0$. We now have$(a) \subseteq q$, since $(a) = q$is possible by the minimality of q. On the other hand$(a\alpha) = a\alpha^2 = a\alpha \neq 0$, here we have$(a) \subseteq q$, since$a\alpha = (a)$. Also $a = ab$for every$b \in \alpha$, and therefore $a = ab = ab^2 = \cdots = ab^r = \cdots$. Hence b$\in \alpha = H^r \supseteq H$, since b is nilpotent and hence we have $a = ab^r = 0$.This contradicts to our choice of a.

Theorem 3.4: *A ring P_i is Artin if an only if P_i is Noetherian and $dim\ P_i = 0$.*

Proof: Initially we know that the $dim\ P_i = 0$. Asume n_i where $1 \leq i \leq r$ will be individual maximal ideals of P_i. Then $\sum_{j=1}^{r} n_i^k \subseteq \left(\bigcap_{j=1}^{r} n_j\right)^k = 0$. Hence by P_i is Noetherian.

Hence the zero ideal as a primary decomposition P_i has exclusively a finite and vary according to stripped prime ideals, hence for all maximal $dim\ P_i = 0$. Since $\bigcap_{j=1}^{r} n_j = 0$ in and P_i is also an Artin ring.

Let P_i is associate Artin ring with high ideal n, then n is that the exclusively prime ideal of P_i so n is that the nilradical of P_i. Since each part of n is nilpotent and n itself is nilpotent. Example of such element is$\frac{W}{p^r}$, where p is prime and such that $r \geq 1$.

IV Symmetry- Assumptions and Generalization on Noncommutative Group

To explain the symmetries, the generalizations on noncommutative cryptography are the subsequent issues on the group G:

(i) Symmetrical Decomposition Problem (SDP):

Given (a, b) ∈G and m, n∈G, find x∈G such that $b = x^m \cdot a \cdot x^n$.

(ii) Generalized Symmetrical Decomposition Problem (GSDP): Given (a, b) ∈G, S⊆G, and x∈Z, find x∈G such that $b = x^m \cdot a \cdot x^n$.

GSDP is clearly a form of restricted SDP, and if the set S is strong enough, then membership data normally doesn't facilitate to extract x from $x^m \cdot a \cdot x^n$. The subsequent GSDP assumption says that it's not versatile to resolve it in probabilistic polynomial time with non-negligible accuracy compared to the dimensions of the problem. This resembles a separate index problem on the group G on single user sign in concepts..

The definition says that prime p to the power $1 + 2n$, that is,p^{1+2n}, has the two properties:

(i) Heisenberg group and semi-direct product of cyclic group order and/or

(ii) Dihedral order 8 and quaternion group.

The quotients or residuals belong to the partof nontrivial whose center is cyclic. Since its size is prime, its classification relies on prime p = a pair of or p = odd. The rationale for this can be clearly that each prime quantity starts with a pair of and also the remaining prime numbers exclusively belong to odd numbers.

The S-USI mechanism for authentication in distributed environments gets benefit from the mathematical properties of Artinian rings. By employing these rings, it’s possible to enhance the security and efficiency of the authentication process. The algebraic structure provided by Artinian rings might contribute to a more secure implementation of S-USI by addressing potential vulnerabilities and ensuring robust performance in practical applications.

V Conclusion

In summary, this study tackles key security and privacy issues in cloud-based, dispersed networks by proposing a novel authentication scheme that utilizes sensors and sensor-tags through a Single-User Sign-In (S-USI) approach. The integration of sophisticated algebraic structures, notably Artinian rings, greatly improves the authentication process and addresses vulnerabilities such as replay attacks, insider threats, mutual authentication concerns, and user anonymity. The rigorous security analysis confirms the strength of the S-USI mechanism, proving its capability to establish a secure and dependable authentication framework. Additionally, the method's comparative analysis highlights its lower computational demands compared to existing alternatives, positioning it as a promising solution for telecare medical information systems. This development marks a significant advancement in enhancing the security and privacy of cloud-based networks in pervasive computing scenarios.

Refrences

[1] M. Aqalmoun, M. El Ouarrachi, Radically principal rings, Khayyam J. Math. 6 (2020), no. 2, 243-249
[2] M. Azrour, J. Mabrouki, A. Guezzaz and Y. Farhaoui, "New enhanced authentication protocol for Internet of Things," in Big Data Mining and Analytics, vol. 4, no. 1, pp. 1-9, March 2021, doi: 10.26599/BDMA.2020.9020010.

[3] Douglas R. Stinson, Cryptography Theory and Practice, Third Edition, Taylor and Francis Group, LLC, 2006
[4] Gautam Kumar, Hemraj Saini, "Novel Noncommutative Cryptography Scheme Using Extra Special Group", Security and Communication Networks, vol. 2017, Article ID 9036382, 21 pages, 2017. https://doi.org/10.1155/2017/9036382
[5] K. R. Goodearl and R. B. Warfield, Jr., An Introduction to Noncommutative Noetherian Rings, Cambridge University Press: Cambridge, Great Britain, 1989.
[6] A. Hamed, S-Noetherian spectrum condition, Commun. Algebra, 46(8), 3314-3321. (2018).
[7] K. A. Ismail, D. E. Dobbs and N. Mahdou, Commutative rings and modules that are Nil∗-coherent or special Nil∗-coherent, J. Algebra Appl., 16(10) (2017), 1750187 (24 pp).
[8] T. F. Lee and C. M. Liu, "A secure smart-card based authentication and key agreement scheme for telecare medicine information systems", J. Med. Syst., vol. 37, no. 3, pp. 1-11, 2013.
[9] Neri, F. (2016). An Overview on Algebraic Structures. In: Linear Algebra for Computational Sciences and Engineering. Springer, Cham. https://doi.org/10.1007/978-3-319-40341-0_7
[10] Suresh Kallam , M K Jayanthi Kannan , B. R. M. , . (2024). A Novel Authentication Mechanism with Efficient Math Based Approach. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3), 2500–2510. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/5722
[11] F. G. Wang and H. Kim, Foundations of Commutative Rings and Their Modules, Algebra and Applications, 22, Singapore, Springer, 2016.