International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Conserving Digital Archaeological Data in Tamil Nadu: Cyber Security Hazards

Dr. E. Iniyan

Assistance Professor of Archaeology, School of Social Sciences
Tamil Nadu Open University, Chennai, Tamilnadu, India
dreiniyan@tnou.ac.in

Abstract
The risk of cyberattacks on the priceless artifacts escalates as Tamil Nadu rapidly digitizes its archeological records, inscriptions, and heritage assets. This article highlights the risks that cultural institutions confront in the digital age by examining the relationship between cybersecurity and digital archaeology. In addition to evaluating the possible effects on Tamil Nadu's archaeological data, it looks at worldwide patterns in cyberattacks on cultural institutions and the dangers of data loss, intellectual property theft, and public access disruption. The essay emphasizes that in order to protect Tamil Nadu's digital legacy, strong cybersecurity infrastructure, employee training, and policy integration are urgently needed. It promotes a future in which technology complements, rather than jeopardizes, the preservation of cultural memory by outlining tactical steps for digital resilience.

Keywords: Digital Archaeology, Cyber Security, Cyber Attack, Data Preservation, Ransomware

Introduction

Tamil Nadu is recognized as one of the most archaeologically abundant regions in India, boasting a cultural legacy that spans thousands of years—from Paleolithic sites and Neolithic communities to the impressive rock-cut temples of the Pallava dynasty, exquisite Chola bronzes, and extensive urban landscapes. However, for a significant portion of the twentieth century, the exploration of this remarkable history depended on conventional techniques: manual surveys, hand-drawn site maps, paper documentation, and physical archives dispersed among various institutions. The processes of documenting, analyzing, and preserving the archaeological treasures of Tamil Nadu were labor-intensive, frequently inaccessible, and susceptible to the effects of time and environmental deterioration. The advent of the twenty-first century has brought about a significant change. Digital technologies—such as remote sensing, Geographic Information Systems (GIS), photogrammetry, 3D modeling, database management systems, and artificial intelligence—are fundamentally altering the ways in which archaeologists uncover, document, analyze, and disseminate knowledge regarding Tamil Nadu's historical narrative. The Digital Turn refers to a transition towards conventional techniques for field survey, excavation, documentation, and interpretation and toward methods that rely on technology and data. For more accurate and efficient information collection, storing, and analysis, archaeologists now use technologies including Geographic Information Systems (GIS), 3D modelling, remote sensing,

digital photography, and database management systems. Ancient settlement patterns and trade networks that were previously unknown to ground surveys have been uncovered by remote sensing technologies, such as satellite photography and LiDAR (Light Detection and Ranging), which have exposed hidden landscapes behind thick vegetation and agricultural fields. By mapping the spatial relationships between urban centres, irrigation systems, and temples, GIS platforms allow academics to provide light on the intricate design that defined about various empires. These days, rock-cut sculptures and inscriptions may be captured in breath taking three-dimensional detail using high-resolution photogrammetry and laser scanning, producing digital twins that can be examined, altered, and conserved even as the originals deteriorate and weather. Significant archaeological discoveries have been made in Tamil Nadu for many years, including the Paleolithic artifacts at Attirampakkam, the huge Iron Age and early historic settlements at sites like Adichanallur, Kodumanal, Korkai, Sivakalai, Porpanaikkottai, and the historic excavations at Keezhadi. These findings, especially those pertaining to the early date of the Iron Age and the usage of the Tamil-Brahmi alphabet, are constantly casting doubt on and changing the chronology of South Indian—and in fact, pan-Indian—civilizational history. This transformation in the digital realm promotes interdisciplinary collaboration among archaeologists, data scientists, and historians, leading to the creation of innovative research frameworks that synthesize field data with computational analysis. Thus, Tamil Nadu's archaeology is evolving into a more inclusive, transparent, and analytically potent structure—connecting historical traditions with future technological innovations. In Tamil Nadu, the amount and importance of digitally-born or digitized archaeological data is growing quickly, mostly due to state-level dedication to modern documentation and large-scale, well-publicized excavations.

Modern field procedures commonly produce GIS layers, LiDAR/photogrammetry point clouds, 3D models and high-resolution digital imagery (photogrammetry) that did not exist a decade ago — so the volume of digital archaeological data (not just scans of paper) is rising fast.[1] A significant shift from paper-based records has been made with the use of 3D modelling (photogrammetry/laser scanning), GIS mapping, and digital databases. Excavations at various locations, specifically Keezhadi, have been considered to be the source of born-digital data acquisition. 3D volumetric precision is used to record each trench, artifact, and feature, producing extremely accurate, long-lasting, and analyzable spatial datasets for the whole site. Research is being done on the application of UAV LiDAR for extensive topographical and subsurface analysis. The extensive legacy data of Tamil Nadu's archives, which includes old excavation reports, historical images, and thousands of stone inscriptions (epigraphy), are being transformed into digital formats that are easily accessible. Because tangible documents were dispersed, it was previously impossible to conduct new, extensive comparative research. Present-day excavations frequently provide materials to scientific laboratories for DNA and material composition analysis, as well as to overseas labs (such Beta Analytic, USA) for dating. The findings, which are essentially numerical and born-digital (e.g., the date for Keezhadi being in the 6th century BCE and the rejection of the Iron Age chronology at Sivagalai), give the archaeological story unquestionable, scientific support. Institutions like the French Institute of Pondicherry and Tamil Nadu Archives collaborate on digitization programs such as the Digital Archive of South Indian Inscriptions (DASI) and the Endangered Archives Project. DASI integrates transcription, translation, and images of Tamil inscriptions, while EAP458 digitized over 10,000 Tamil agrarian records and temple manuscripts, preserving endangered primary sources.[2]

Preserving the Fragile Past of Tamilnadu in a Digital Future

From ancient inscriptions and temple architecture to unearthed artifacts and manuscripts, Tamil Nadu's rich archaeological and cultural legacy is constantly in danger from human activity, time, and climate change. As a result, digital preservation has emerged as a key tactic for protecting this heritage. By constructing digital archives, generating 3D scans of monuments, and scanning delicate documents, scholars guarantee that priceless cultural information is always available for future research and public education. Digital tools are being used by organizations like the Archaeological Survey of India and the Tamil Nadu State Department of Archaeology to record and preserve cultural assets. Digital preservation thus creates a lasting digital legacy for future generations while simultaneously preventing the loss of the tangible past. The Archaeology Policy Note 2024–2025 outlines state-driven goals to digitize excavation reports, documentary archives, and temple inventories as part of a broader digital heritage infrastructure.[3] With the assistance of a ₹10-crore state allocation, the Tamil Nadu Archives, which was recently acknowledged as a national model, has digitized over eight lakh historical records utilizing cutting-edge Japanese tissue mending and digital imaging technology. These initiatives are in line with national missions like Abhilekh Patal and the National Mission on Monuments and Antiquities (NMMA), which work together to establish centralized digital repositories of India's historical assets. The Roja Muthiah Research Library (RMRL) in Chennai leads microfilming and digitization of 19th- and 20th-century publications related to Tamil Nadu's social, religious, and political movements. These materials, including early literature on Vaishnavism, Saivism, Christianity, and Dravidian politics, are preserved under the Endangered Archives Programme to prevent deterioration. Their approach uses both microfilm and high-resolution digital TIFF images, balancing traditional archival practice with modern longevity.[4] Predictive modeling for conservation needs, automated transcription of ancient inscriptions, and pattern identification for archaeological surveys are all made possible by AI algorithms. Artifact dating and authenticity can be aided by machine learning's ability to recognize stylistic trends in architecture and art. Tamil-specific natural language processing techniques are being developed, which could allow for the automated examination of large textual datasets. The public can participate in heritage preservation through digital channels. People can add local knowledge, oral histories, and photos to shared databases. Thousands of photos of Tamil Nadu's historical places have been contributed by volunteers all around the world to websites like Wikimedia Commons. The artificial intelligence models have been trained using a bespoke dataset of damaged temple murals gathered from locations such as Thiruvalanchuzhi's Kapardeeswarar Temple, Tanjore's Brihadeeshwarar Temple, Kumbakonam's Ramaswamy Temple, and Kanchipuram's Kailasanathar Temple. The system is effective in recreating huge parts of naturally damaged murals, as evidenced by its superior quantitative findings with Mean Squared Error, Peak Signat to no Noise Ration, Learned Perpetual Image Patch Similarity values, and Structural Similarity Index Measure. Traditional methods like bilinear and bicubic interpolation only average pixel values, often resulting in blurry or grainy visuals. AI models, on the other hand, enhance image quality by predicting new pixel data, preserving fine details, and reducing noise.[5]

Uncommon Hurdles Encountered within Tamil Nadu's Archaeological Landscape

With its prehistoric settlements, megalithic burials, urban centers from the Sangam era, and medieval temple complexes, Tamil Nadu has one of the most abundant archeological landscapes in South Asia. Adichanallur, Keezhadi, Porpanaikkottai, Sivakalai, Kodumanal, and Korkai are only a few

of the locations that highlight the lengthy history of human habitation and sociocultural development. However, a number of administrative, technological, and environmental limitations make it difficult for the area to preserve, research, and interpret its extensive archaeological record. The tropical climate of Tamil Nadu, marked by high humidity, monsoonal rainfall, and fluctuating temperatures, accelerates the decay of organic and metallic artefacts**.** Erosion, flooding, and salinization in coastal sites (e.g., Poompuhar) threaten stratigraphic layers and context integrity.[6] Despite the growing global usage of tools like GIS, remote sensing, photogrammetry, and 3D modelling, their use in Tamil Nadu archaeology is still restricted to a few academic projects. Digital archaeology and AI-based analysis are not widely used because of a shortage of skilled interdisciplinary workers who combine data science and archaeology. Most archaeological remains in the state are extremely vulnerable because they are not centrally or state-protected, especially smaller megalithic sites, prehistoric rock art, and hero stones. The absence of strong security makes these locations prime targets for theft, vandalism, and illegal relic hunting, especially of metal idols and sculptures from partially damaged or unprotected temples that are being trafficked overseas. Increased public awareness and community involvement are essential to addressing this negligence. When compared with government agencies like department of archaeology and archaeological survey of India, the other institutions like universities which has the archaeology departments are lagging with inadequate fund and staff to carry out the excavations. Though exploration is carried out throughout the state by various scholars, cultural preservationists and heritage lovers, common concept of acquiring material remains through excavation is not being done by the agencies responsible for archaeological research. Another important aspect here to be noticed is the allotment of necessary fund for the archaeological research is not substantiated. Inadequate awareness programmes conducted among the public regarding the preservation of archaeological resources is also another cause for the destruction of material remains.[7]

The man-made disturbances are the serious cause for the destruction of ancient archaeological remains. Necessary technological advancement should be implemented at the heritage sites and the use of computer modelling to simulate the impact of future climate change should be effectuated in those areas. A comprehensive research work should be under taken to analyse the effects of changes occurring in the water quality due to the alteration in the climatic condition and in addition to this the maintenance of anoxic environment is influenced by the micro-organisms present on them which are sensitive to minute changes in the water properties. Excessive rainfall pouring at present and in coming days and drying following it, results in the alteration of cli mate and initially influencing the stratigraphic condition known from the cracking and heave due to the penetration of oxygen leading to the rapid microbial action and oxidation of metals and other artefacts in the layers of the trench.[8]

Cyber-security Hazards

The confidentiality, integrity, and availability (CIA) of priceless cultural heritage data are at risk due to serious cyber-security threats to Tamil Nadu's digital archaeological data protection. These risks are exacerbated by the special significance and frequently constrained resources of heritage organizations, as well as general weaknesses in digital infrastructure. In order to maintain the long-term integrity of cultural data, Tamilandu has to implement rigorous cyber defense measures as it accelerates its digital conservation efforts through DigiArchives and digitized inscriptions and item databases. Historical relics, excavation reports and sensitive site maps are frequently found in digital collections. These may be prone to illegal access or leaks in the absence of strong access controls. The government

released Cyber Security Policy 2.0 in August 2024, updating the decade-old framework to combat new attack vectors faced by state agencies and public sector units. This policy, created with input from the Centre for Development of Advanced Computing (C-DAC), IIT Madras, and the Tamil Nadu e-Governance Agency, sets strict guidelines for audit, compliance, and monitoring.[9] Data can be encrypted and held hostage by ransomware, which can affect organizations digitizing archaeological data. Threats from ransomware and phishing attacks have increased for the state's public sector, particularly as digital governance grows. Dedicated cyber-security infrastructure and skilled staff are lacking in many archaeological and historical organizations. In the absence of appropriate risk classification for digital assets, important archaeological data might not be adequately safeguarded. International sharing of digital heritage data increases the risk of its exploitation for political or economic ends.

Future research may be misled and scientific credibility compromised by computer hacking that change 3D reconstruction files or metadata. Even slight data errors in archaeology might lead to incorrect stratigraphic, chronological, or artifact classification conclusions. The adoption of cloud-based digital repositories by Tamilnadu State Department of Archaeology and other heritage initiatives increases the danger of data leaks (sensitive research data pertaining to excavations, artifacts, or digital heritage archives that is inappropriately used, lost, or exposed without authorization), improperly configured permissions which may enable unauthenticated people to access, duplicate, or modify protected archaeological data, posing a danger of site looting, data manipulation, or breaches of information that is sensitive to the community (such as data about sacred or Indigenous heritage) and third-party breaches (which occurs when a third-party vendor, contractor, or service provider with access to sensitive archeological data but insufficient security measures allows the data to be hijacked. Even if these breaches take place outside of the main research institution's own IT infrastructure, they can nevertheless have a major negative impact by disclosing private information like artifacts, researcher credentials, or excavation records) particularly when cloud services do not adhere to ISO/IEC 27001 standards. As far as the mitigation strategies are concerned implementing multi-factor authentication and encryption for all digital archives, conducting regular cyber-security audits and vulnerability assessments, educating employees on danger awareness and digital hygiene is very much necessary.

Digital Archaeological Landscape of Tamil Nadu

The immense archaeological legacy of Tamil Nadu is documented, examined, and preserved through the collection of born-digital and digitized material known as the Digital Archaeological Landscape of Tamil Nadu. An comprehensive digital archive of Tamil Nadu's past is being created with the help of these sources, which include museums, academic institutions, archaeological departments, GIS-based surveys, and digital heritage initiatives. The state's principal repository for archaeological data is the Tamil Nadu State Department of Archaeology (TNSDA), which creates online heritage inventories, 3D artefact records, photographic documentation, and digital excavation reports. Digitizing the state museum collections, Adichanallur artifact catalogues, and Keezhadi excavation archives are some of TNSDA's recent projects. The Tamil Nadu State Archives contain digitized copies of records from the colonial period, administrative papers, and unique historical manuscripts. These digital collections offer historical insights into archaeological sites and cultural traditions.

The universities and research institutions in Tamil Nadu have a significant role to generating born-digital archaeological data by means of surveys, fieldwork, and digital analysis. Department of Ancient History and Archaeology, University of Madras conducts GIS mapping**,** ceramic typology databases**,** and digital cataloguing of artefacts, Tamil University in Thanjavur specializes in digital epigraphy**,** digitization of palm-leaf manuscripts**,** and heritage informatics related to Tamil civilization, School of Earth and Atmospheric Sciences, Madurai Kamaraj University in collaboration with other institutions has a history of conducting geospatial studies in the region, focusing on land use, natural resource management, and water bodies. This expertise in Geographical Information Systems (GIS), the technology that relies on DTMs, lays the foundation for archaeological applications. MKU also in collaboration with Liverpool John Moores University in England used advanced forensic and genetic analysis, including facial reconstruction, on remains from the Keezhadi archaeological site, another instance of leveraging high-tech tools for archaeological study. Roja Muthiah Research Library (RMRL), maintain digital repositories of archaeological literature, excavation reports, historical photographs, and fieldwork documentation. The analysis of settlement patterns, trade networks, cultural transformations, and site discoveries can be aided by techniques such as supervised and unsupervised learning, statistical modeling, big data analytics, and digital preservation strategies. Specifically, machine learning and digital visualization have been applied to Tamilnadu's rich archaeological context, including Keezhadi and other Sangam-age settlements, in order to classify inscriptions, date artefacts, and reconstruct past landscapes. Archaeology, heritage management, and public history are linked through data science, thereby fostering interdisciplinary collaboration.[10] Archaeological Survey of India (ASI) – Chennai Circle provides satellite mapping, 3D scanning, and photogrammetric surveys of protected sites across Tamil Nadu and the National Mission on Monuments and Antiquities (NMMA) hosts digital inventories and maps of archaeological sites across the state.

Data Integrity and Authenticity Threats

Digital formats like databases, 3D models, GIS maps, and digital archives are currently used to record and preserve a large portion of Tamil Nadu's archaeological research, which includes excavations at Keezhadi, Adichanallur, Korkai, and Kodumanal. Information preservation is aided by this digital transformation, but data authenticity and integrity are also at stake. Threats to data integrity arise from the loss, alteration, or corruption of archaeological data as a result of technical malfunctions, illegal manipulation, or file deterioration. The scientific value of the original data may be lost, for instance, if digital records of artifacts or site coordinates are inadvertently altered or compromised. When the originality or source of data is unknown, such as with edited photos, phony datasets, or missing information, authenticity risks occur. This may undermine the reliability of research and result in inaccurate interpretations of Tamil Nadu's archaeological legacy. To guarantee that the digital records of Tamil Nadu's rich history continue to be accurate, verifiable, and reliable, safeguarding archaeological data in the state necessitates secure digital storage, appropriate metadata documentation, version control, and cyber-security precautions.

Inaccurate historical reconstruction, misdated artifacts, or manipulated site maps can result in inaccurate interpretations of Tamil Nadu's ancient civilizations, like those at Keezhadi or Adichanallur, among others. Intentional falsification can also tamper with digital records to support political or cultural agendas or promote biased historical narratives. Weak cyber-security in heritage institutions can permit

unauthorized edits or deletions, particularly in open-access databases or poorly protected archives. If metadata and documentation are lost or changed, the provenance and context of artifacts are obscured, compromising their academic and cultural value. It is imperative that archaeological research employ certain mitigation strategies to prevent data alteration. These strategies include implementing version control and audit trails for all digital records, using block-chain or cryptographic hashing to ensure data integrity, educating staff members on digital ethics and secure data handling, and working with cyber-security experts to protect heritage databases. There are serious risks to Tamil Nadu's archaeological data records from unintentional or deliberate harm to data files during processing, storage, or transfer. Damage of this kind may result in the partial or complete loss of important historical material, including site maps, excavation reports, inscriptions, and artifact metadata. In accidental damage data corruption is caused by hardware failures, software glitches, improper backup procedures, or human errors during file handling. Unstable storage media or interrupted data transfers can introduce file inconsistencies, leading to irreversible loss of digital archives if not detected early.[11] Deliberate deletion, alteration, or sabotage of archaeological data files can occur due to insider threats or external cyberattacks aiming to manipulate historical narratives or disrupt research continuity. In Tamil Nadu, political controversies around site interpretations like Keezhadi have heightened concerns about intentional interference with digital records.[12]

Due to the increasing digitization of Tamil Nadu's archaeological records, which include sites such as Keezhadi, Porpanaikkottai, Adichanallur, Kodumanal, Mayiladumparai, Kilnamandi, Korkai, and others, a significant amount of sensitive data, such as inventories of artifacts, site coordinates, excavation reports, and researcher details, are now digitally stored. The digital transformation raises serious privacy and data confidentiality issues. Inappropriate sharing or access to sensitive archaeological data, such as precise site locations or unpublished excavation data, can result in confidentiality problems and expose researchers to dangers including illicit artifact trafficking, site vandalism, or abuse of research data. When field reports, internal communications, or personal information are made public because of inadequate cyber-security or a lack of data governance, privacy concerns also impact researchers and partner organizations. Ensuring that only authorized scholars and heritage authorities handle digital archaeological data responsibly requires the establishment of cyber-security frameworks, ethical sharing standards, and data access restrictions in order to preserve Tamil Nadu's historical legacy. [13] The vulnerabilities to sensitive information about Tamil Nadu's archaeological data are substantial and can be categorized into three main types namely physical vulnerabilities (like looting), digital vulnerabilities (linked to cyber-security), and administrative or political vulnerabilities (due to mismanagement). As far as Physical vulnerabilities are concerned unprotected sites might be vulnerable when specific locations, such as Keezhadi, Kodumanal, Sivagalai, etc., are made public, as well as the type of high-value finds (such as gold, rare artifacts, and detailed site maps). Smugglers would then use these sites to target unexcavated areas, permanently destroying historical context and artifacts. The digital vulnerabilities includes large-scale digital datasets created by data science, GIS, and 3D modelling, combined with poor cyber-security or archiving, can result in the loss of priceless digital records (such as scientific dating reports or excavation layers) or their unapproved leak, which exacerbates physical risks like site encroachment. The administrative or political vulnerabilities comprises of data integrity and release might be jeopardized by political pressures, non-standardized data formats, and documentation delays. The archaeological findings from

Tamil Nadu at several locations are historically noteworthy. For commercial or strategic purposes, individual collectors or foreign organizations may try to obtain unapproved access to excavation data, site coordinates, or unpublished findings. Digital records of artifacts, cultural maps, and academic publications are susceptible to unauthorized use and plagiarism. Lack of appropriate copyright safeguards puts local academics and organizations at risk of having their work taken over by international publishers or for-profit websites. A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack inundates a server or network with an overwhelming amount of traffic, rendering it unreachable for authorized users. This can lead to either temporary or permanent interruptions in access to archaeological databases, digital libraries, or research portals. Such incidents can hinder access to excavation records, GIS maps, and cultural heritage databases, causing delays in research and digital preservation efforts. In particular cases, attackers may aim at heritage institutions to solicit ransom or to obstruct cultural documentation initiatives. It is imperative to strengthen cyber-security infrastructure, firewalls, and backup systems to protect Tamil Nadu's digital archaeological data from these types of disruptions. Hardware malfunction and storage medium deterioration pose threats to Tamil Nadu's digital archaeological records, potentially leading to the irreversible loss of priceless excavation data and historical archives. Data corruption or unreadable files result from the deterioration of magnetic cassettes, CDs, and hard drives over time. This deterioration is further accelerated by poor maintenance and environmental factors like dampness. To maintain long-term data integrity, regular data migration, cloud backups, and digital preservation techniques are crucial. Researchers have identified several threats to the longevity, integrity, access and quality of the digital information storage. Some of these are Media decay and failure, Bit rot, Outdated media, Massive storage failures, Network failure, Access component obsolescence, Outdated formats, Applications and systems failure, Natural Disasters, Human and Software errors, External attacks, Insider attacks, Economic failure, Organizational failure, Politics and Censorship.[14] The changes in the format of coding had a great impact in the digital world which initially has a influence in Tamilnadu archaeological data storage. Archaeological research in Tamil Nadu focuses significantly on digital preservation since it guarantees the long-term accessibility and preservation of excavation records, inscriptions, artifact photos, and GIS data. By preserving the usability and authenticity of digital cultural resources, it aids in preventing data loss from environmental deterioration, cyber threats, and device failure. It also enables future study. Tamil Nadu's rich cultural legacy is protected for scholars and future generations through effective digital preservation. A significant concern in the management of digital archaeological data from Tamil Nadu is accidental erasure. Unintentional deletion of crucial excavation records, 3D site models, or inscription databases can happen as a result of human error, software bugs, or poor system management. Research continuity may be disrupted and precious cultural information may permanently vanish as a result of such losses. In order to avoid and recover from unintentional deletions, it is imperative to have user access protocols, version control, and regular data backups. It has been recognized by the Tamil Nadu State Department of Archaeology and Tamil Nadu Archives that irreversible data loss in excavation reports, GIS mapping layers, and digitized palm-leaf manuscript collections is increased by inadequate backup scheduling and a lack of version control. Digital preservation units prioritize automatic version tracking, regular cloud backups, and limited administrator access to prevent repetition. These measures assist reduce unintentional deletions in long-term archaeological data storage. Another important factor responsible for the authenticity threat is the technological obsolescence, reason being the inability to access data due to outdated hardware or software formats. Lack of awareness and training and the insufficient cyber-

security knowledge among archaeological professionals is the other reason for authenticity threat in Tamilnadu archaeological records. Phishing and social Engineering to exploit human trust to gain unauthorized access is the other factor.

The administration and interpretation of Tamil Nadu's digital archaeological data are heavily influenced by geopolitical and ideological factors. These incentives frequently influence how historical narratives and excavation results are presented, managed, or shared online. An advanced, indigenous, and early urban civilization that predates or is contemporaneous with early North Indian traditions is speculated to be proven by major excavations, notably at sites like Adichanallur, Keeladi, Kodumanal, Sivakalai, Porpanaikkottai, etc. Digital data helps to authenticate and spread this claim to a larger audience, both scientific and popular, by making evidence readily available and verifiable (e.g., carbon dating results, artifact photos, site plans). Tamil Nadu's Dravidianist political ideology, which emphasizes a distinct, non-Sanskritic cultural stream in South India, frequently characterizes the findings. Digital platforms turn into a tool for counter-narratives, which use data that appears to be scientific to support assertions of an autonomous cultural trajectory that contradicts stories of a single, Northern-centric Indian civilization. Deliberate attacks on digital heritage of Tamilnadu by groups seeking to erase or manipulate historical narratives also poses a great threat in the conservation of Tamilnadu heritage.

Current State of Cyber-security Preparedness in Tamil Nadu's Archaeological Institutions

The laws and infrastructure currently in place in Tamil Nadu archaeology demonstrate a strong framework supported by substantial government commitment and cutting-edge scientific methods that aims to preserve and investigate the state's rich cultural legacy. Digital resources like GIS databases, remote sensing data, 3D models, online archives, etc., are becoming more and more important in Tamil Nadu's archaeological study. Yet, the cyber-security architecture that underpins these systems is frequently weak or dispersed, devoid of reliable firewalls, secure servers, or uniform access restrictions. There are currently few explicit recommendations for digital data protection, user authentication, or data backup processes, instead, they primarily concentrate on site protection and physical legacy management. Because of this, archaeological datasets—such as inscriptions, excavation records, and GIS maps—are vulnerable to ransomware attacks, illegal access, and data breaches. To protect Tamil Nadu's digital historical heritage, it is essential to strengthen cyber-security regulations, put digital preservation standards into practice, and carry out routine infrastructure audits. The point we have hopefully been driving home is that digital repositories and archives, besides facing physical destruction, are also vulnerable to cyber-security threats during times of conflict. The chaos and instability inherent in physical and information warfare creates opportunities for malicious actors to exploit digital weaknesses. The intentional targeting of digital heritage has become a real and pressing concern. Hacking, data breaches and cyber-attacks on digital libraries can result in the manipulation, theft or destruction of cultural artifacts.[15]

Cyberattacks that focus on digital archaeological archives are a threat that archaeologists in Tamil Nadu are less cognizant of yet. In contrast to digital security and cyber-security procedures, which are yet not fully structured for archaeological education or institutional regulations, training and experience primarily concentrate on fieldwork, excavation, and artifact preservation. Sensitive information, including inscriptions, GIS maps, excavation records, and 3D models, may therefore be

susceptible to ransomware attacks, illegal access, or data breaches. The state's digital history must be protected, and this requires raising awareness through cyber-security training, digital literacy initiatives, and institutional policies. The Tamil Nadu Government has unveiled Cyber Security Policy 2.0, which replaces the earlier iteration from 2020. This new policy delineates precise guidelines aimed at securing the government's digital systems and ensuring their protection.

In the Tamil Nadu State Department of Archaeology, funding for strong cyber-security measures seems to be limited and not specifically designated for digital protection. Given its incomparable significance and susceptibility, Tamil Nadu's archaeological data need strong cyber-security promptly. The most significant record of an ancient civilization is archaeological information, such as site coordinates, artifact measurements, carbon-dating results, and photographic documentation. The loss is permanent if this digital data is hacked. Data could be corrupted or discreetly changed by a cyberattack (e.g., changing dates or coordinates). This would lead to inaccurate interpretations of Tamil Nadu's past and irreversibly falsify history while also jeopardizing the integrity of the research. A whole digital archive might be encrypted by a ransomware assault, thereby locking away important knowledge about the ancient Sangam-era culture and preventing researchers, historians, and the general public from accessing it. Strong cyber-security would make that the Tamilnadu State Archaeology Department follows these laws and regulations. Mission-critical historical assets that shape national and cultural narratives are the discoveries made at different excavated locations. Protecting this data is essential to safeguarding the state's intellectual property and cultural legacy against nefarious actors and politically driven attempts to falsify historical records. Research institutions like Universities and cultural heritage institutions are the subject of cyberattacks, especially those with geopolitical intent that aim to foment conflict by falsifying historical facts or disturb a country's cultural identity. The use of sophisticated digital tools such as GPR, UAV, LiDAR, and GIS for documentation in Tamil archaeology increases the volume and complexity of data, posing additional risks that need to be addressed by staff training, ongoing vigilance, and state-of-the-art security infrastructure.

Strategies and Best Practices for Cyber-security in Tamilnadu Digital Archaeology

Safeguarding the state's rich cultural legacy and assuring the long-term accessibility of archaeological records depend heavily on comprehensive data management and preservation in Tamil Nadu's digital archaeology. In conjunction with digitization projects like the Tamil Nadu e-Governance Agency's DigiArchives project (Digital Archives of Tamil Nadu (DigiArchives) is an initiative of Tamil Nadu e-Governance Agency (TNeGA). It provides a platform to aggregate and provide the archived artifacts that are available with the different Departments in the State in digital format, neatly organized as archives with customized categories, sorted by Year, with keywords to easily search and view / download the artifacts with secure access. The project is hosted on state-of-the-art infrastructure to support multi-tenancy for more Departments to publish their archives and for people to access them with ease),[16] the Tamil Nadu State Department of Archaeology has put in place structured policies and infrastructure to ensure that archaeological data is documented in a methodical manner, stored securely, and has standardized metadata. In data acquisition and documentation standard, standardized data format should be captured in non-proprietary and archival-friendly formats in the form of images of file names as TIFF or JPEG at higher resolution (300-1200 dpi) in addition to the open formats like ASCII (American Standard Code for Information Interchange) CSV (Comma Separated Values - each line

represents a row in this plain-text file format, and values inside a row are separated by a delimiter, usually a comma. ex. "Name","Age","City","Alice",30,"New York", "Bob",25,"Los Angeles") for long term preservation. To prevent cataclysmic loss, data should be archived in redundant, secure digital repositories with safe on-site and off-site backups. To ensure accessibility as technology advances, a strategy ought to be in place to periodically move data to more recent, reliable file formats or media. The procedure frequently entails keeping a derivative format for modern usage, the original supplied format, and a preservation format (such as ASCII CSV for spreadsheets). Digital curators must be employed by the repository to ensure that data is complete, of high quality, and that archiving guidelines are followed. In order to ensure that material is accessible while adhering to ethical and legal restrictions, repositories must also offer controlled access (e.g., sensitive site information).

Redundant backups with multiple copies stored in geographically diverse locations (on-site, off-site, cloud), adherence to International Digital Preservation Standards (e.g., OAIS Reference Model, PREMIS) should be adapted. Metadata standards and version control in ensuring detailed, consistent metadata and tracking all changes, implementation of strong technical security measures, multi-factor authentication, granular access permissions and encrypting data at rest and in transit, regular security audits and vulnerability assessments are much needed strategies to be adapted. Monitoring for malicious activity, protecting sensitive personal data where applicable, developing a cyber-security culture, cyber-security training for all personnel handling digital archaeological data, clear procedures for detecting, responding to and recovering from cyber incidents, documented guidelines for data handling, storage, and access, proper legal and policy frameworks, compliance with data protection laws (e.g., India's Digital Personal Data Protection Act – DPDP Act 2023 - depending on whether the data is "personal data" in a digital format, regulations governing the processing of digital personal data and its application to heritage data will be prioritized) are also important in preserving the digital archives of Tamilnadu heritage. DPDP despite focusing more on personal information than cultural or archaeological information, it has significant ramifications for Tamil Nadu's heritage management. Adherence to the DPDP Act guarantees that personal identifiers in digital archives, excavation records, or heritage surveys are gathered and handled legally, openly, and securely for archaeological and heritage organizations. National and State-Level Strategies with the development of specific policies for cultural heritage data security, international and inter-institutional collaboration, sharing best practices and threat intelligence, joint development of secure digital repositories are important in the cyber-security procedures to be followed to protect the Tamilnadu archaeological digital data’s. This process will enhance the understanding of need for the necessity of cyber-security measures to be implemented in preserving the digital archaeological records of Tamilnadu history.

Cyberattack on Cultural Heritage Institutions Globally and its possible Impact on Tamilnadu Archaeology

Cyberattacks targeting the digital infrastructures of museums, archives, libraries, and archaeological sites have become a rising global issue. These assaults frequently seek to use ransomware to extort a ransom, interfere with operations, or steal confidential information. Common types of cyberattack includes Ransomware (encrypts digital collections, archives, financial, and HR data), Data Breach (Targets patron data (personal, financial, and donation history), staff HR files (social security numbers, tax info), and confidential collection information (provenance, appraisals)., Supply Chain

Attack (Allows hackers to gain access to multiple cultural institutions simultaneously, causing widespread outages and data theft across the sector), Denial of Service (Disrupts public-facing online services, research access, and critical functions like ticket sales), Phising and Social Engineering (Often the initial entry point for a ransomware attack, exploiting human error) and State Sponsored Espionage (Targets national libraries and archives to steal or manipulate intellectual property and sensitive political or cultural records).

Many prominent museums and cultural institutions worldwide have been victims of ransomware, where hackers lock digital archives or systems and demand payment for release. For example, the U.S. Cleveland Museum of Art faced ransomware attacks disrupting collection access in 2023,[17] In 2024 several major museums using the software company gallery Systems (used for collections management) were impacted in a cyber-incident that disrupted access to digital collections, provenance data, etc. Recent cyber attacks on cultural institutions, including the Internet Archive, national libraries (London Public Library, Calgary Public Library, various libraries in British Columbia, the Toronto Public Library), as well as national museums in Europe and North America, go beyond simple ransom attempts and represent a significant threat to democratic resilience and cultural preservation.[18]

By jeopardizing the security, accessibility, and integrity of priceless digital archaeological material, cyberattacks on cultural heritage organizations can have a serious effect on Tamil Nadu archaeology. With its enormous digital archives and archaeological sites, Tamil Nadu is susceptible to cyberthreats that could interfere with public outreach, heritage management, and investigation. Potential impacts of cyberattacks on Tamilnadu archaeology comprises of loss of irreplaceable data's like digitized excavation reports, inscriptions, and historical manuscripts could be corrupted, deleted, or held ransom erasing years of scholarly work and cultural memory, losing the high-quality records of 3D Scans and High-Resolution Images would compromise future virtual conservation and research, critical data's from Carbon-14 dating, chemical preservation, and metallurgical analysis that support the claim of earlier Iron Age in Tamil Nadu could be subjected to cyberattack. The loss or corruption of this specific data could make it impossible to scientifically defend the historical and chronological significance of the Keezhadi findings, effectively setting back years of monumental research. Manipulation of data integrity includes alteration of key records, erosion of trust which would leads to the misconception of authenticity of the Tamil Antiquity. The recent scientific dating records and the archaeological finds (Keezhadi, Porunai, Sivagalai, and Mayiladumparai) in Tamil Nadu have garnered a lot of national and international attention. Because of its prominence, the related data is a more alluring target for threat actors with political or financial motivations. With the introduction of the Cyber Security Policy 2.0, Tamil Nadu has demonstrated its proactive approach to cyber-security. But the threat still exists, as seen by the ransomware attack on the state's Public Department in 2021, which exposed flaws like the installation of antiquated operating systems and inadequate cyber hygiene. Archaeology is one of the several state departments that may be vulnerable. Due to the department's rapid accumulation of priceless digital material due to the push for digitization and the sheer volume of artifacts being found, the stakes for a breach are extremely high. Since archaeology in Tamil Nadu is increasingly dependent on digital technologies and e-governance platforms, protecting against hackers is

crucial. Tamil Nadu's archaeological data may be protected from changing cyberthreats by incorporating cutting-edge cyber-security solutions, employee training, frequent audits, and policy enforcement.

Conclusion

A multidimensional, proactive approach is needed to secure Tamil Nadu's digital archaeological future. This approach must take into account the special importance and sensitivity of cultural heritage data, such as the excavation records, in addition to implementing the state's current Cyber Security Policy 2.0. Prioritizing cyber-security by designating archaeological data systems as important digital infrastructure and requiring cyber-security audits for all digital platforms utilized by the state archaeology department should be the primary concern for the purpose to further safeguard archaeological data. Network segmentation serves as essential for segregating the network which comprises primary excavation data (such as field notes, 3D scans, and C-14 reports) from the systems that are visible to the public (such as websites and online libraries). It should be inconceivable for an attacker to access the key research data if they manage to compromise the public site. Protecting the archaeological data requires the use of Role-Based Access Control (RBAC) to limit access to the data. To give an example, a museum curator solely needs access to their antiquity catalogue not the core server logs—to site an exhibit. To further enhance Tamilnadu's digital archaeological future, emphasis should be placed on implementing blockchain or version-controlled systems to monitor changes in digital records and using redundant backups across secure cloud and physical servers. Ensuring safe access to sensitive data through multi-factor authentication and implementing firewalls, intrusion detection systems, and encryption techniques are also the main concerns in the process of protecting Tamilnadu archaeological data from potential hacking threats. Archaeologists, researchers, and museum employees in Tamilnadu can benefit from training on digital literacy and cyber-security to increase their understanding of cyber threats and the need of preserving the future of digital archaeology. As required by the Cyber Security Policy 2.0, it is also necessary to formally nominate a dedicated team of officials from the Tamilnadu State Department of Archaeology that will collaborate directly with the Cyber Security Incident Response Team (CSIRT) of Tamil Nadu. Furthermore, all contractors and third parties involved in the digitization process have to go across mandatory security audits and follow the stringent security clauses of the Cyber Security Policy 2.0, as they are a common vector for breaches in the government sector. In the present context, the development of scientific technology and computational techniques that support archaeological research, such as artificial intelligence, would greatly aid in promoting Tamilnadu archaeological data and preserving it for future generations to view virtually and make it appear realistic. Therefore, in order to improve the robustness and credibility of digital archives, Tamilnadu archaeological research must embrace cutting-edge solutions like blockchain based tamper-proof ledgers, secure cloud services, and AI-driven anomaly detection. Promoting the inclusion of funds specifically allocated to digital heritage security in the state's archaeological budgets, supported by proactive government initiatives that combine IT security frameworks with heritage preservation is very much appreciated in the cyber-security process of Tamilnadu digital Archaeology future.

Proactive cyber-security is essential in order to preserve Tamil Nadu's digital archaeological resources in an era when technology and legacy coexist. A single breach might wipe out priceless cultural memory as the state digitizes centuries of history. In addition to being technically necessary,

proactive investment in secure infrastructure, employee training, and policy integration demonstrates a dedication to preserving Tamil Nadu's legacy for coming generations.

Reference

1. **Sivanantham, Ramesh Masethun, Ajay Kumar Ramamoorthy et.al.,** Applications and their Archaeological Inferences - Keeladi Excavations, Reflections on Cultural Development: An Archaeological Perspective (Ed), Chapter 112, November 2023, p.112-128
2. **Ebeling, Sascha,** "The Digital Archive of South Indian Inscriptions (DASI) — A First Report". South-Indian Horizons, edited by Jean-Luc Chevillard and Eva Wilden, Institut Français de Pondichéry, 2004, https://doi.org/10.4000/books.ifp.7841.
3. **Policy Note 2024-2025,** Archaeology, Tourism, Culture and Religious Endowments Department, Government of Tamilnadu.
4. Roja Muthiah Library | Preserving Tamil Heritage
5. **Thinking Stack,** https://www.thinkingstack.ai
6. **Selvakumar, V,** Environmental Challenges in South Indian Archaeology, Indian Journal of History of Science, 53(2), 2018, 225–234
7. **Dr. E. Iniyan,** Remnants of Archaeology at Risk in Tamilnadu – Defending Tamilnadu's Hidden Heritage, IJRAR, Vol.5, Issue.4, 2018, p. 600-605.
8. **Dr. E. Iniyan,** Alteration in Climatology and its exigency in conserving the Archaeological sites in Tamilnadu, Essays on Archaeological Studies (ed), Che Publishing House, 2018, p.64-81.
9. https://codesecure.in, Government Cybersecurity: Tamil Nadu Public Sector Protection
10. **Dr. E. Iniyan,** The Implications of Data Science in Contemporary Tamilnadu Archaeological Interpretation, RESEARCH HUB International Multidisciplinary Research Journal, Vol.12, Issue.9, September 2025,
11. **Sudipta Shee,** Digital Preservation of Cultural Heritage in India: A Digital Age, International Journal of Humanities and Education Research, Vol.7, Issue.1, 2025, p.260-265.
12. **V. Prathiyukshaa, Mr.Akhil Jobel,** A Study on Current Trends in Cybercrime and its Targeted Victim Building Cybersecurity Practices and Awareness, International Journal of Research and Analytical Reviews, Vol.12, Issue.2, May 2025, p.929-953.
13. **Kumar, K. V.**, Digital Transformation and Risk in South Indian Heritage Management, Indian Archaeological Review, 12(2), 2021, p. 89–102.
14. **Mani M. Manivannan,** Very long-term digital preservation and archival strategies for Tamil documents, Academia
15. **Christina Dinh Nguyen**, Digital cultural heritage in the crossfire of conflict: Cyber threats and cyber-security perspectives, UKSG Insights, Vol.37, May 2024.
16. https://tnega.tn.gov.in
17. Digital Application in Archaeology and Cultural Heritage, **Elsevier**
18. https://greydynamics.com, cyber-attacks-on-cultural-institutions-heritage-under-siege