# Using Blockchain to Prevent Ransomware Attacks


**Student Researchers**

**Aaliyah Lockett, Alocket7@students.asurams.edu**
**Shamar Swift, Sswift@students.asurams.edu**

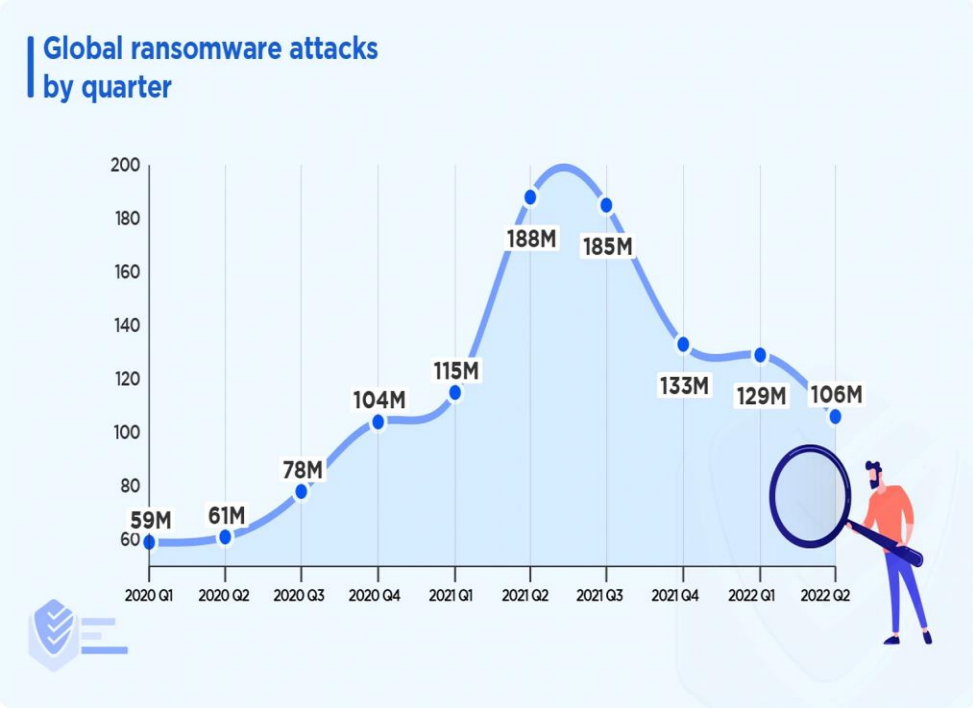
**Faculty Advisors**
**Dr. Robert Steven Owor, Robert.owor@asurams.edu**
**Ms. Amiralca Johnson, Amiralca.johnson@asurams.edu**

**Albany State University, 504 College Drive, Albany, GA 31705**


Albany State University
University System of Georgia

# Abstract

- Ransomware has emerged as a major cyber threat, transforming into a lucrative criminal enterprise. Many victims find paying the ransom the only viable option to retrieve their data.
- This not only perpetuates the cycle but also funds future attacks. We propose a blockchain-based solution involving multiple proxy servers and a control server, ensuring data integrity and facilitating swift response to ransomware attacks



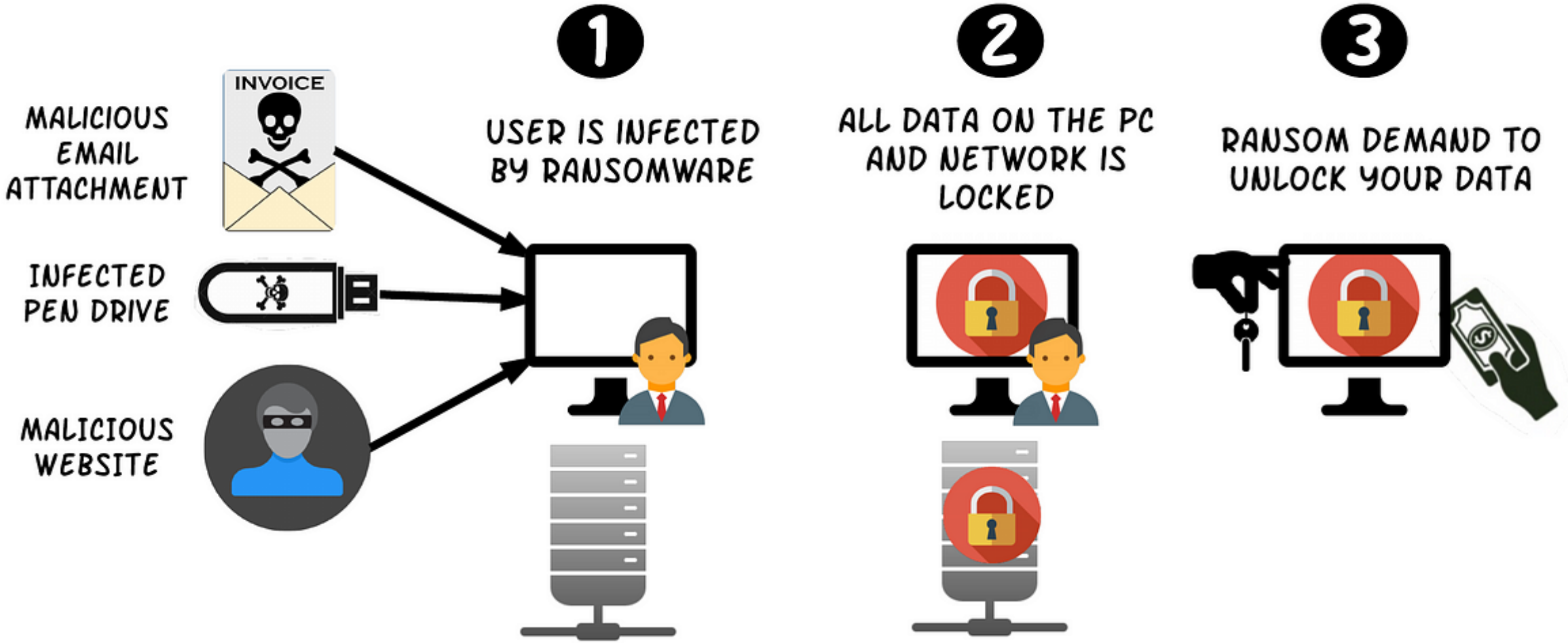
# Abstract (Continued)

- Every business that pays to recover its files inadvertently supports the evolution of more sophisticated ransomware. Our solution employs blockchain technology to record identical transactions across multiple servers. If one server is compromised, it is isolated, and operations continue seamlessly with a new server setup. This method ensures continuous protection and facilitates investigation into the attack's origin.

# Introduction

- Ransomware is malicious software that encrypts files, demanding a ransom for their decryption. This form of cybercrime targets high-profile entities, demanding payment usually in bitcoin due to its anonymity. Failure to pay results in permanent data loss.

# HOW RANSOMWARE WORKS?



# Scareware


- Scareware involves fake security software and tech support scams, bombarding users with pop-up alerts claiming malware detection. Users are coerced into paying to remove the non-existent threat. Tracking scareware operators can involve monitoring their IP addresses and Bitcoin transactions.

# Screen Lockers


- Screen lockers prevent users from accessing their computers, displaying a message purportedly from a government agency, alleging illegal activity and demanding a fine. Legitimate agencies do not operate this way.

# Encryption Ransomware

- Encryption ransomware locks users' data, demanding payment for decryption. Victims face data loss even after payment. A robust solution involves using multiple servers to ensure data redundancy and quick recovery.

# Mobile Ransomware

- Mobile ransomware targets smartphones, locking them or stealing data. Regular backups to the cloud can mitigate this threat, allowing users to restore data to a new device if attacked.

# Sample Cases of Ransomware Attacks: City of Dallas Attack

- **Description**: The Royal ransomware group targeted municipal services in Dallas, Texas, on May 2023. The attack primarily affected the IT systems and communications of the Dallas Police Department.
- **Impact**: Network printers started printing ransom notes, causing significant operational disruptions.
- **Aftermath**: The city had to invest in recovery and mitigation efforts to restore services and enhance cybersecurity measures (Kaspersky).

# Sample Cases of Ransomware Attacks: MOVEit Transfer Attack

- **Description**: On June 2023, the Clop ransomware group exploited a vulnerability in the MOVEit Transfer tool by Progress Software. This attack affected numerous organizations globally, including several in the U.S.
- **Impact**: Notable U.S. victims included the New York City Department of Education and the University of Georgia. The attack disrupted operations and compromised significant amounts of data.
- **Aftermath**: The incident highlighted the critical importance of timely patching and vulnerability management across organizations (Kaspersky).

# Sample Cases of Ransomware Attacks: Caesars and MGM Casinos Attack

- **Description**: On September 2023, the ALPHV/BlackCat ransomware group attacked two major U.S. hotel and casino chains, Caesars and MGM.
- **Impact**: The attack crippled the companies' infrastructure, affecting everything from hotel check-in systems to slot machines. While Caesars chose to pay the ransom, MGM faced operational shutdowns.
- **Aftermath**: The incident led to a reevaluation of cybersecurity strategies in the hospitality and entertainment industries(Kaspersky) (DNI).

# Sample Cases of Ransomware Attacks: Prospect Medical Holdings Attack

- **Description**: The Rhysida ransomware group targeted Prospect Medical Holdings, on August 2023, which operates multiple hospitals and clinics across several states.
- **Impact**: The group stole 1TB of corporate documents and a 1.3TB SQL database containing sensitive personal and medical records, demanding a ransom of 50 BTC (approximately $1.3 million).
- **Aftermath**: The attack caused significant disruptions in medical services and exposed vulnerabilities in healthcare cybersecurity (Kaspersky).

# What is a Blockchain

- Blockchain is a decentralized ledger that records transactions in blocks, linked together in a chain. Each block's integrity is ensured by the previous block's hash, making data tampering nearly impossible.
- Blockchain's key principles include integrity, immutability, and decentralization. Data is distributed across all network nodes, eliminating a single point of failure and ensuring continuity even if a node is compromised.
- Decentralization ensures that no central server can be attacked to bring down the system. In the event of a ransomware attack, affected nodes can be restored or removed without disrupting the entire network.

# Blockchain as a Solution for Ransomware

- While Bitcoin is often used for ransomware payments, blockchain technology can counteract these attacks. Its decentralized and immutable nature makes it an ideal defense mechanism.

# Modex BCDB

- Modex BCDB enables easy integration of blockchain technology into existing systems without extensive technical knowledge. It combines blockchain with traditional databases, offering robust security without requiring developers to learn new skills.

# Modex BCDB Benefits

- Modex BCDB simplifies blockchain adoption, making it accessible for businesses. It fuses blockchain's security features with database familiarity, allowing seamless integration and enhanced data protection

# Modex BCDB Implementation

- Modex BCDB's middleware approach allows developers to use blockchain technology without altering their existing workflows, providing a straightforward path to enhanced security.

# Conclusion

- Blockchain technology, exemplified by Modex BCDB, offers a powerful defense against ransomware. By leveraging blockchain security features, businesses can protect their data and maintain operational integrity even in the face of cyber threats.

# References


- Afraz, N. "Is blockchain a friend or foe in ransomware attacks?" Silicon Republic, last accessed May 20, 2022.
- IBM Cloud Team. "Prevent ransomware attacks with blockchain." IBM Blog, last accessed May 20, 2022.
- Newsweek Staff. "The Rise in Ransomware: Here's How to Fight It." Newsweek, last accessed May 20, 2022.
- Sokolov, K. "Ransomware activity and blockchain congestion." University of Memphis, Fogelman College of Business and Economics, 2022.
- Akcora, C. G., Li, Y., Gel, Y. R., & Kantarcioglu, M. "Bitcoin Heist: Topological Data Analysis for Ransomware Detection on the Bitcoin Blockchain." June 2019.
- Mosakheil, J. H. "Security Threats Classification in Blockchains." St. Cloud State University, May 2018.
- Institute for Security and Technology. "Combating Ransomware." Ransomware Taskforce, 2022.