European Journal of Computer Science and Information Technology, 14(6),16-34, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Cloud Data Security Techniques for Payment Card Systems: A Review of Cryptographic and Blockchain-Based Approaches

Joel Abakah Hagan[1], **J.B. Hayfron-Acquah**[2], **Dennis Redeemer Korda**[3]*, **Obeng Owusu-Boateng**[4], **Nelson Seidu**[5], **Eric Ayintareba Akolgo**[6]
[1]Department of Computer Science, Takoradi Technical University, Takoradi, Ghana. Email: joelhagan30@gmail.com
[2]Department of Computer Science, Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana
[3]Department of Computing & Information Technology, Bolgatanga Technical University, Bolgatanga, Ghana
[5&6]Department of Computer Science, Regentropfen University College, Bolgatanga, Ghana.
[4]Department of Mathematics & ICT, E. P College of Education, Ghana.
*Corresponding email: mawugbe4@gmail.com

doi: https://doi.org/10.37745/ejcsit.2013/vol14n61634 Published September 27, 2026

Citation: Hagan J.A., Hayfron-Acquah J.B., Korda D.R., Owusu-Boateng O., Seidu N., Akolgo E.A. (2026) Cloud Data Security Techniques for Payment Card Systems: A Review of Cryptographic and Blockchain-Based Approaches, *European Journal of Computer Science and Information Technology*, 14(6),16-34

Abstract: *With the exponential growth of payment card transactions, the global shift from cash to digital payments has intensified, and the Payment Card Industry (PCI) has embraced cloud computing for its scalability and efficiency. Traditional cloud storage systems, however, rely on trusted third-party providers, which can result in centralized storage, high costs, and trust concerns. This review examines a wide range of literature on cloud computing, cloud security and trust, e-commerce risk, and cryptographic techniques relevant to the protection of payment card data stored and shared in the cloud. It surveys the rise of cloud computing and its service and deployment models, the security issues and attack vectors that affect cloud-based systems, the role of phishing in payment card fraud, and the influence of perceived risk on consumers' online purchase intention and trust. It further reviews cryptographic techniques used to secure cloud data, including symmetric and public-key encryption, searchable encryption, homomorphic encryption, and attribute-based cryptography (encryption, signatures, and signcryption), before examining blockchain technology as a decentralizing mechanism for cloud trust. A comparative analysis of existing cloud data security protocols is presented, showing that Attribute-Based Signcryption (ABSC) offers the most comprehensive coverage of confidentiality, integrity, availability, authenticity, and access control relative to Attribute-Based Encryption (ABE) and Attribute-Based Signatures (ABS) used independently. The review concludes that blockchain-integrated attribute-based signcryption is a promising direction for decentralizing trust in cloud-stored payment card data, but that such constructions require rigorous, formally verified security analysis before deployment, since at least one prominent scheme has been shown to be insecure.*

Keywords: cloud computing; payment card security; cryptography; blockchain; attribute-based signcryption; perceived risk; phishing

INTRODUCTION

With the exponential growth of payment card transactions, the global shift from cash to digital payments has intensified. The Payment Card Industry (PCI) has embraced cloud computing, drawn to its scalability and efficiency. Traditional cloud storage systems rely on trusted third-party providers, which can result in centralized storage, high costs, and trust concerns. Security has always been one of the key challenges in cloud computing, and its usage and implementation would continue to increase if this challenge were addressed (Alam, 2020). One of the challenges that have to be addressed in order to alleviate some of these barriers is security requirements. As a result of certain other technical resources, cloud computing offers many benefits since it can process and store large amounts of data as well as provide other services. Cloud computing platform decreases service costs and deals with problem of limited resource and space by sharing essential resources among different users. But at the same time, cloud computing platform has to cope with new security threats since this is the key for ensuring performance of the platform.

This review explores a variety of literature that is highly relevant to cloud computing, cloud security and trust, e-commerce, encryption techniques and more. It explores the emergence of cloud computing, the danger associated with e-commerce, the role of phishing attacks in payment card fraud, risk perception and purchase intention, and cryptographic technique reviews, before synthesizing existing cloud data security protocols in a comparative analysis. The objective is to consolidate the current state of knowledge on securing cloud-stored payment card data and to identify the technical direction — attribute-based signcryption integrated with blockchain — that best satisfies the combined requirements of confidentiality, integrity, availability, authenticity, and access control (CIAAA) in cloud-based payment systems.

THE RISE OF CLOUD COMPUTING IN THE PAYMENT CARD INDUSTRY

The cloud data storage and retrieval mechanism is a commonly used system. Rather than coming up with their own mechanisms, several companies such as the PCI have opted for cloud services, which they utilize in a pay-as-you-go (PAYG) or membership mode (El Alloussi, Fetjah & Chaichaa, 2014). Over the past few years, the concept of cloud computing has become one of the most crucial concepts in computing. Cloud computing has developed into a significant invention that will significantly affect internet services generally as well as the information technology sector overall. Its creation optimizes the accessibility of software, hardware, and data on demand in order to realize economies of scale in both the delivery and administration of IT efforts (Alam, 2020).
Research on cloud security has concentrated mainly on software security, data storage security, and network security (Ali, Khan & Vasilakos, 2015; Singh, Jeong & Park, 2016). The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort (Mell & Grance, 2011). Its essential characteristics are on-demand self-service, broad network access,

resource pooling, rapid elasticity, and measured service; the last of these underpins the PAYG model, in which users pay only for the resources they actually consume (Mell & Grance, 2011). Virtualization is used to deliver these pooled resources to users efficiently. Despite these advantages, many businesses remain reluctant to adopt cloud technologies, with security and trust as principal concerns (Ali, Khan & Vasilakos, 2015; El Alloussi, Fetjah & Chaichaa, 2014).

Cloud Service Delivery Models

New service models emerge as big data, cloud computing, and internet technology develop, and these new services can provide connections among the ever-expanding array of online activities. The three principal delivery models identified in the literature are as follows.

NIST identifies three service models (Mell & Grance, 2011). Infrastructure as a Service (IaaS) provides consumers with processing, storage, networking, and other fundamental computing resources, typically accessed through APIs on a pay-per-use basis, on which they can deploy and run arbitrary software, including operating systems; Amazon EC2 is a well-known example. Platform as a Service (PaaS) provides a cloud-hosted development and deployment environment in which databases, web servers, programming languages, and tools are shared resources, so developers can build applications without managing the underlying infrastructure (Pham et al., 2017); Microsoft Azure App Service and Google App Engine are examples. Software as a Service (SaaS) delivers complete applications, such as email, office productivity, and design tools, on demand to many clients from a provider-managed cloud environment; Google Workspace, Microsoft 365, and Salesforce are examples. Beyond these three models, the term 'Anything as a Service' (XaaS) is used informally for further offerings such as Data as a Service and Security as a Service.

Cloud Deployment Models

Cloud computing relies on the pooling and sharing of resources among users, and NIST identifies four deployment models (Mell & Grance, 2011). A private cloud is provisioned for the exclusive use of a single organization and may be managed by that organization or by a third party. A community cloud is provisioned for a specific community of organizations with shared concerns such as mission, security requirements, policy, and compliance; it can lower the cost of a private cloud while reducing the exposure of a public cloud. A public cloud is provisioned for open use by the general public and may be owned and operated by a business, academic, or government organization; because its resources are shared with unknown tenants, strong service level agreements (SLAs) between provider and customer are needed to maintain mutual confidence. A hybrid cloud is a composition of two or more of these infrastructures that remain distinct entities but are bound together by standardized or proprietary technology that enables data and application portability (Mell & Grance, 2011). A virtual private cloud, which is not one of the NIST models, is an isolated, configurable pool of resources carved out of a public cloud and usually accessed through a virtual private network (VPN).

Cloud Security Issues and Challenges

The security posture of the cloud environment spans a variety of fields with notable vulnerabilities, with trust identified as a significant issue influencing customer behaviour (Ali, Khan & Vasilakos, 2015; Singh, Jeong & Park, 2016). Table 1 summarizes representative attacks affecting cloud service models and their corresponding countermeasures drawn from the reviewed literature.

Table 1. Representative cloud attacks and countermeasures (adapted from Singh, Jeong & Park, 2016; Ali, Khan & Vasilakos, 2015)

Attack	Affected Cloud Service(s)	Representative Countermeasures
Authentication	SaaS	Stronger authentication and strong passwords; encrypted communication channels for safe authentication tokens; federated identity secured via extensible access management and assertion markup standards
Denial of Service (DoS)	SaaS | PaaS | IaaS	Signature-based detection strategies; layered authorization and authentication; intrusion detection/prevention systems
Phishing	SaaS | PaaS | IaaS	Safe web links; spotting scam emails; avoiding dubious or unfamiliar URLs
SQL Injection	SaaS	Proxy-based structures to identify and sanitize user input; avoiding dynamic SQL in coding
Man-in-the-Middle	SaaS | PaaS | IaaS	Strong encryption/decryption algorithms; secure socket layer architecture; intrusion detection systems
Port Scanning	SaaS | PaaS | IaaS	Firewalls; time-independent features; neural networks and packet-count analysis
Cross-VM Attack	IaaS	Virtual firewalling; encryption and decryption
Metadata Spoofing	SaaS | PaaS	Encrypting service-functionality metadata; strong authentication for data access
VM Escape	IaaS	Hypervisor activity monitoring; virtual machine isolation; safer hypervisors; host/guest interaction controls
VM Roll-back	IaaS	Suspend-and-resume technique

RISK IN E-COMMERCE AND THE ROLE OF PHISHING IN PAYMENT CARD FRAUD

The widespread adoption of e-commerce has significantly increased the use of payment cards for online transactions and, correspondingly, fraudulent attempts, making accurate fraud prevention an important concern in a cashless economy. Fraud detection techniques such as data mining and

machine-learning-based behavioural analysis are used to supplement primary checks on transactions (Delamaire, Abdou & Pointon, 2009); however, where third-party services are involved, the data on which they rely may itself be exposed to attack. Online payment transactions pass between the client, the merchant's service system, and back-end payment systems, and these exchanges must be protected to ensure the integrity and confidentiality of transaction details and to deter eavesdropping and manipulation.

Credit card use is one of the most popular means of financial transactions today, and the rise in this transactional trend has also increased the rate of credit card fraud and forgery, leading to substantial losses globally (Nilson Report, 2022). Credit card fraud can occur through lost or stolen cards, exposure of personally identifiable information (PII), and phishing attacks (Delamaire, Abdou & Pointon, 2009). Phishing is an identity theft method that seeks to obtain PII — including usernames, credit card numbers, dates of birth, driver's licence numbers, social security numbers, and online passwords — using technology spoofing and social engineering to trick users into disclosing sensitive information (Banu & Banu, 2013). Phishers usually distribute large numbers of formulated emails with links that redirect users to fraudulent sites designed to steal sensitive information that can be used to achieve a payout from a victim's account, or design web pages that mimic legitimate sites requesting personal or sensitive information.

According to industry data, gross payment card fraud losses worldwide reached US$32.34 billion in 2021, an increase of 13.8% on 2020, and rose further to US$33.83 billion in 2023 (Nilson Report, 2022; Nilson Report, 2025). Recognized types of credit card fraud include application fraud, in which a card account is obtained using false or stolen personal details; counterfeit fraud, including skimming, in which data captured from a card's magnetic stripe are used to produce a cloned card; and card-not-present fraud, in which stolen card details such as the account number, expiry date, and CVV are used for remote purchases without the physical card (Delamaire, Abdou & Pointon, 2009). Phishing has also extended beyond email to telephone and SMS channels, and techniques such as email and web spoofing, malware, and DNS cache poisoning are employed to conduct phishing attacks (Banu & Banu, 2013).

PERCEIVED RISK, FEAR OF IDENTITY THEFT, AND ONLINE PURCHASE INTENTION

Perceived risk is a crucial driver of consumer behaviour during online credit card transactions and is a major factor affecting internet commerce today. It can be defined as the level of risk associated with using the internet to make transactions, data privacy, and general cyber-environment unpredictability. Online purchase intention is the decisiveness to make a move, or a stage of conceptualization during decision-making, where the customer acquires an actual willingness to follow a particular brand or item; a rise in purchase intention indicates a rise in the likelihood of completing a purchase, though whether a consumer accepts or rejects a product is ultimately determined by their intent (Jordan, Leskovar & Marič, 2018).

Consumer trust and long-term customer relationships are generally regarded as being influenced by reputation, which is built through sustained investment of time, attention, and resources in customer relationships. Consumers tend to choose companies with a good online reputation because it reduces their perception of risk (Kim & Lennon, 2013). Trust in the online vendor is therefore central to e-commerce, since it lowers perceived risk and encourages positive feedback and recommendations. When a customer communicates with an e-vendor online and provides private information, the customer is in a vulnerable position, presuming that the vendor's website is a safe platform and that the vendor will fulfil the purchase request competently while preserving the confidentiality and integrity of the customer's data (Jordan, Leskovar & Marič, 2018).

Fear, among other emotions such as joy, anger, sadness, disgust, acceptance, surprise, and expectation, is one of the major emotions people experience, and the fear of identity fraud has been described as a new unpleasant customer emotion triggered by customers' own ideas about the risk of personal, sensitive, and financial information theft when making online purchases (Hille, Walsh & Cleveland, 2015). Two aspects of online identity theft are fear of losing money and fear of damaged reputation: First, the fear that unauthorized entities are accessing and using personal financial data to make them money in an illegal or unethical manner causing financial damage when stolen confidential information is used to make purchases without the victim's permission; Second, the concern about personal data being obtained in an unauthorized way and used for impersonation which may result in a damage to the victim's reputation. Past literature suggests that there are three hypotheses to be explored: (1) fear of financial loss positively correlates with perceived risk; (2) fear of reputational damage positively correlates with perceived risk; and (3) online purchase intention negatively correlates with perceived risk (Jordan, Leskovar & Marič, 2018). Thus, consumers' increased risk perceptions act as a barrier to purchasing intent, and the relationships among identity theft anxiety, perceived risk, and purchasing intent have been examined several times in the literature by conceptual models based on these hypotheses.

CRYPTOGRAPHIC TECHNIQUES TO SECURE CLOUD DATA

Cryptography is the science of designing codes that secure data and communications, and encryption is its core process. Key management is crucial, since if a key is compromised an attacker gains access to all data protected by it; in many cloud deployments, key management falls primarily to the Cloud Service Provider (CSP). Because users cannot always verify how a CSP handles their data, client-side cryptographic techniques also protect users against a CSP they do not fully trust (Ali, Khan & Vasilakos, 2015). Using cryptographic techniques increases security at the cost of performance, and the appropriate balance depends on the user, the required performance, and the level of security sought.

The functionalities of cryptography relevant to cloud environments include the ability to search encrypted data without full retrieval and decryption; control of storage, whereby users retain governance over where their data is stored; access control, the limitations placed on data access;

and data computation, which allows (at a cost) calculations to be performed on data that would otherwise require full decryption first.

Foundational Protocols: RFC 2401–2404

RFC 2401 establishes the base security architecture that secures IP-layer (IPv4 and IPv6) traffic, offering access control, data-origin authentication, connectionless integrity, replay protection, encryption, and traffic-flow confidentiality, and employs the Security Association (SA) construct to manage and implement IPsec interoperability (Kent & Atkinson, 1998a). RFC 2402 defines the IPsec Authentication Header (AH) protocol, which achieves data integrity, origin authentication, and replay protection, and can be used independently, alongside the Encapsulating Security Payload (ESP), or in tunnel mode (Kent & Atkinson, 1998b). The Message Digest 5 (MD5) algorithm and HMAC are defined in RFC 2403 for AH and ESP, which processes data in 64-byte blocks and truncates the 128-bit HMAC-MD5 output to a 96-bit authenticator value (Madson & Glenn, 1998a; Rivest, 1992). RFC 2404 describes the same approach, using the Secure Hash Algorithm (SHA-1), whose 160-bit HMAC output is likewise truncated to 96 bits (Madson & Glenn, 1998b), which ensures that the packets sent in transit are genuine and unaltered by either sender or receiver if both parties possess the shared HMAC key.

Encryption Approaches

Cryptography converts plaintext into ciphertext that can be understood only by authorized parties. Symmetric-key encryption requires both parties to share the same key for encryption and decryption (Cai & Yao, 2022), and the Advanced Encryption Standard (AES) is the most widely deployed symmetric algorithm (NIST, 2001). In this area, Ghanaian cloud security research has contributed a two-level cryptographic solution that uses the symmetric AES together with asymmetric Elliptic Curve Cryptography (ECC) to encrypt data as it transits to cloud storage, reducing cryptographic processing time and improving data confidentiality and integrity against intruders (Hodowu, Korda & Ansong, 2020). Akobre, Wiredu, Daabo and Agebure (2025) introduced a hybrid RNS-AES encryption scheme in Cipher Block Chaining mode with HMAC-SHA256 for authenticated data protection in cloud and IoT environments, balancing the competing requirements of strong security and low processing time. Public-key (asymmetric) encryption uses a key pair — a publicly available key and a secret private key — so that the sender encrypts with the recipient's public key and only the recipient can decrypt with the corresponding private key; RSA is the most widely used realization of this method (Rivest, Shamir & Adleman, 1978). Hybrid schemes such as that of Hodowu, Korda and Ansong (2020) combine symmetric and asymmetric algorithms to obtain strong security with faster processing than asymmetric encryption alone.

Searchable encryption encrypts data before it is stored in the cloud while still allowing the server to search over the ciphertexts when specific information is required. Symmetric searchable encryption, introduced by Song, Wagner and Perrig (2000), uses a single secret key and enables the data owner to search encrypted cloud-stored data for specific keywords. Asymmetric searchable encryption, known as public-key encryption with keyword search (PEKS), supports

multiple-writer, single-reader scenarios in which anyone can encrypt data under the reader's public key while only the holder of the private key can generate search trapdoors (Boneh et al., 2004).

Homomorphic encryption enables computation on encrypted data without prior decryption; the resulting computations remain encrypted and yield, once decrypted, the same result as if the computation had been performed on the plaintext. Partially homomorphic encryption permits only one operation type (addition or multiplication) at a time. Somewhat homomorphic encryption permits a constrained number of operations, since allowing more would generate noise that alters the original data structure. Fully homomorphic encryption supports arbitrary computation, typically by evaluating circuits built from XOR and AND gates, which correspond to addition and multiplication over bits; although its security is high, it remains very time consuming (Chillotti et al., 2020). This is a fundamental trade-off between the level of security desired and the computational cost involved. In the space, Korda, Ansong and Hodowu (2021) presented a variant of homomorphic encryption that performs computations on scrambled data stored in the cloud without requiring the customer to give up a secret key to the cloud server, known as the SDC algorithm, and tested it with big-O analysis and the Python-based SDC library, demonstrating satisfactory correctness and efficiency and providing some supporting evidence that homomorphic approaches could be made practical for real cloud deployments instead of remaining purely theoretical.

Attribute-Based Cryptography: ABE, ABS, and ABSC

The encryption is called Attribute-Based Encryption (ABE), the idea of which originates from Fuzzy Identity-Based Encryption (FIBE), which substituted identities with a collection of descriptive attributes (Sahai & Waters, 2005). ABE encrypts the ciphertext not for a single user, but for a set of authorized users, and includes the user's private key and the ciphertext with attribute structures so that only an authorized user whose private key meets the access policy mentioned in the ciphertext can get the cleartext (Goyal et al., 2006). There are two basic kinds: Key Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) (Goyal et al., 2006; Bethencourt, Sahai & Waters, 2007; Waters, 2011). Subsequent research has introduced constant-ciphertext-length variants to reduce communication costs (Chen, Zhang & Feng, 2011; Emura et al., 2009), lightweight pairing-free ABE for the Internet of Things (Yao, Chen & Tian, 2015), and outsourced computation to improve efficiency given the linear complexity of pairing computation in most ABE schemes.

Attribute-Based Signatures (ABS) apply cryptography as both a cipher and a digital signature, guaranteeing confidentiality, integrity, and immutability, and are typically required for user authentication when accessing cloud services. Only if the attributes of a user match a certain access policy granted by an attribute authority to a user, a user may sign a message using an attribute-based signature. Only the parameters required of the attribute-based signature are publicly accessible while the attributes and secret keys are generated by an attribute authority (Maji, Prabhakaran & Rosulek, 2011). ABS schemes need to be both private (conceal the signer's identity and attributes) and unforgeable (even if the signer colludes with others, it would be impossible to

produce a signature that breaks the access constraints), and can be classified as multi-authority and single-authority based on the level of authority involvement (Li et al., 2010).

Attribute-Based Signcryption (ABSC) combines the benefits of encryption and digital signatures in a single logical step, originally proposed as digital signcryption by Zheng (1997), and is realized in attribute-based form by logically combining ABE and ABS. ABSC offers ciphertext unforgeability, data confidentiality, integrity, proper authentication, and trustworthy access control, while requiring less computation time than the conventional encrypt-then-sign approach. A number of ABSC-based cloud data-sharing schemes have been proposed for health-record protection (Liu, Huang & Liu, 2015; Rao, 2017), with some later shown to fail to achieve claimed data confidentiality or public ciphertext verification, prompting refined constructions validated under the decisional bilinear Diffie–Hellman random oracle model. More recent schemes fuse blockchain technology with attribute-based signcryption to remove the trusted third-party storage provider (Eltayieb et al., 2020); however, subsequent cryptanalysis showed that this blockchain-based construction is not secure against confidentiality attacks (Li et al., 2022), underscoring the need for formally verified designs.

Table 2 summarizes the coverage of the core cloud data security requirements — Confidentiality, Integrity, Availability, Authenticity, and Access Control (CIAAA) — by ABE, ABS, and ABSC as reported in the reviewed literature.

Table 2. Comparative coverage of cloud data security requirements by ABE, ABS, and ABSC (compiled from Goyal et al., 2006; Maji, Prabhakaran & Rosulek, 2011; Liu, Huang & Liu, 2015; Rao, 2017)

Technique	Confidentiality	Integrity	Availability	Authenticity	Access Control
ABE	✓	—	✓	—	✓
ABS	—	✓	✓	✓	—
ABSC	✓	✓	✓	✓	✓

As Table 2 illustrates, while cloud data is always readily available for retrieval by the user, ABE alone satisfies confidentiality and access control, and ABS alone — through its reliance on digital signatures — assures integrity and authenticity. Combining both into ABSC produces a more robust mechanism that jointly ensures confidentiality, integrity, availability, access control, and authenticity, which is why ABSC is regarded in the reviewed literature as the most complete of the attribute-based primitives for securing cloud-stored payment card data, provided that the specific construction used has been rigorously proven secure (Li et al., 2022).

European Journal of Computer Science and Information Technology, 14(6),16-34, 2026
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

TECHNOLOGY OF BLOCKCHAIN AS A CLOUD SECURITY ENABLER

Blockchain technology was introduced by Nakamoto (2008) in the white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System', which described an electronic cash system allowing payments to be made directly between parties without a trusted third party. Transactions are recorded on a shared, append-only ledger: participants can add new transactions, but altering a recorded one would require redoing the proof-of-work of that block and all subsequent blocks. Blocks are cryptographically linked, each containing the hash of its predecessor, and every full node holds a copy of the transaction history, which provides integrity and high availability; Bitcoin uses the SHA-256 hash function (Nakamoto, 2008). Blockchain has since been generalized beyond cryptocurrency to many other applications (Zheng et al., 2017). Drawing on this design, three fundamental components of blockchain can be identified: a replicated ledger that records all transactions and is copied to every participant; cryptography, which secures the authenticity and integrity of transactions and the identities of participants; and a consensus mechanism that validates transactions and keeps the replicated ledgers consistent.

Public blockchains are permissionless: anyone can join, submit transactions, and take part in consensus, with Bitcoin as the best-known example. They provide an ordered, immutable transaction record but require considerable processing power and, being openly accessible, expose a larger attack surface. Private blockchains are permissioned: participation is controlled by an operator who determines which nodes may submit and validate transactions and read the ledger, which allows faster validation and restricted access at the cost of greater centralization; consortium blockchains, operated by a group of organizations, lie between the two (Zheng et al., 2017).

Blockchain Data Structure and Consensus

The blockchain is a time-stamped transaction history of the entire system, replicated as a shared ledger across a distributed network of nodes. Transactions are gathered into blocks that are appended in chronological order, and once a block is sufficiently deep in the chain, altering it becomes computationally infeasible. A cryptographic hash function produces a fixed-length output from input data of any size and is a one-way function because it is computationally hard to reverse. Each block header contains the hash of the previous block, linking the chain back to the first (genesis) block, together with a Merkle root: a single hash that summarizes all of the transactions in the block through a Merkle tree (Nakamoto, 2008; Zheng et al., 2017).

Blockchain systems run on a peer-to-peer network in which nodes are interconnected without a central authority. Agreement on the state of the ledger is reached through a consensus mechanism: Bitcoin uses proof-of-work, in which nodes accept the longest valid chain, while other blockchains use alternatives such as proof-of-stake or practical Byzantine fault tolerance (Nakamoto, 2008; Zheng et al., 2017). The Merkle tree is not a consensus mechanism but a data structure: because any change to a transaction changes the Merkle root and therefore the block hash, it allows nodes to detect tampering and to verify that a transaction is included in a block without downloading the

whole block (Nakamoto, 2008). Together, hash chaining, Merkle trees, and consensus make the blockchain ledger tamper-evident.

Blockchain Applications in Cloud Trust and Payment Security

A substantial body of work has applied blockchain to cloud trust problems. Blockchain-based applications face trade-offs between decentralization, scalability, and throughput, and because recorded decisions are irreversible, an adversary who controls a majority of the network's computing power can rewrite recent history and double-spend; this majority (51%) attack is one of the most studied threats to public blockchains (Saad et al., 2020).

BPay is a blockchain-based framework for secure and fair payment of outsourced cloud services that does not rely on any third party, trusted or not; it is compatible with both the Bitcoin and Ethereum blockchains and was shown experimentally to be computationally efficient (Zhang et al., 2021). Other work reduces reliance on trusted third parties for data governance, giving users greater control over their data and over who may access them (Al Omar et al., 2019), for example by enforcing access rules through smart contracts on the Ethereum network (Wood, 2014). The Deep Blockchain Framework (DBF) combines collaborative intrusion detection, using a Bidirectional Long Short-Term Memory (BiLSTM) deep learning model evaluated on the UNSW-NB15 and BoT-IoT datasets, with Ethereum-based smart contracts that preserve the privacy of the distributed detection engines, and it outperformed peer privacy-preserving intrusion detection techniques (Alkadi et al., 2021). Liang et al. (2017) proposed a blockchain-based architecture for data provenance in cloud auditing which protected user anonymity and increased data availability by providing an immutable, timestamped blockchain receipt for every data record, and showed that little overhead was associated with provenance in a private cloud. A Blockchain-based Searchable Public-key Encryption scheme with Forward and Backward privacy (BSPEFB) has also been proposed in which a smart contract replaces the central search server, providing forward and backward privacy without relying on a central authority (Chen et al., 2020). In the payment card sector, blockchain has been examined for payment card systems (Godfrey-Welch et al., 2018), and blockchain-based two-factor authentication for credit card validation has been proposed as a way to decentralize trust (Mercan et al., 2022). Olorunshola, Okoroafor and Enem (2025) developed HappyPay, a payment gateway deployed on the Polygon Mumbai testnet that uses smart contracts and integrates MetaMask and WalletConnect wallets to address the centralized control, data breaches, and high transaction fees of conventional payment gateways, reporting fees as low as 0.70 Nigerian Naira per transaction and average processing times of about 4 seconds. Collectively, the studies reviewed in this section evaluate blockchain-integrated cloud systems mainly in terms of cost, performance, and dependability.

COMPARATIVE SYNTHESIS AND RESEARCH DIRECTION

Most existing payment solutions for cloud services are designed for a particular type of service and rely on a trusted third party to ensure fair payment, and mutual distrust between customers and service providers over online payment and data security may impede the wider adoption of cloud

services (Zhang et al., 2021). Across the reviewed literature, individual cryptographic techniques address only part of the combined CIAAA requirement: encryption schemes (symmetric, public-key, searchable, and homomorphic) primarily target confidentiality and, in the searchable and homomorphic cases, controlled computation over protected data; ABE targets confidentiality and access control; and ABS targets integrity and authenticity. ABSC, by logically combining ABE and ABS, is the only reviewed technique that addresses all five requirements simultaneously in principle, and its integration with blockchain can further decentralize the trust anchor away from a single third-party provider, addressing the centralization, cost, and trust concerns identified at the outset of this review. However, the confidentiality attack on the blockchain-based ABSC scheme of Eltayieb et al. (2020) demonstrated by Li et al. (2022) shows that such designs must be formally analysed before they can be relied upon for payment card data.

Table 3 summarizes thirty of the key studies examined in this review, grouped from cloud and consumer-risk foundations through cryptographic primitives to blockchain-based applications, together with the principal contribution of each and the limitation or gap most relevant to securing cloud-stored payment card data.

Table 3. Summary of key studies reviewed

S/N	Author(s) (Year)	Focus / Technique	Key Contribution	Limitation / Gap
1	Mell & Grance (2011)	Cloud computing definition (NIST SP 800-145)	Defines cloud computing through five essential characteristics, three service models and four deployment models.	Definitional; prescribes no security mechanism.
2	El Alloussi, Fetjah & Chaichaa (2014)	Payment card data in the cloud	Examines the issues and perspectives involved in protecting payment card data hosted in cloud environments.	Predates blockchain and attribute-based signcryption approaches.
3	Ali, Khan & Vasilakos (2015)	Cloud security survey	Surveys cloud security issues across communication, architecture, and contractual/legal dimensions together with proposed solutions.	General cloud focus; not specific to payment card data.
4	Singh, Jeong & Park (2016)	Cloud security survey	Classifies threats and attacks by affected service model and maps them to countermeasures.	Countermeasures are catalogued rather than comparatively evaluated.
5	Banu & Banu (2013)	Phishing	Reviews phishing attack types, delivery channels and techniques used to steal personal and card information.	Descriptive; no detection model is evaluated.
6	Hille, Walsh & Cleveland (2015)	Consumer behaviour	Develops and validates a scale measuring consumers' fear of online identity theft.	Measures fear; does not examine technical safeguards.

S/N	Author(s) (Year)	Focus / Technique	Key Contribution	Limitation / Gap
7	Jordan, Leskovar & Marič (2018)	Perceived risk and purchase intention	Survey of 190 participants shows fear of financial loss and of reputational damage raise perceived risk, which lowers online purchase intention.	Single-country (Slovenian) sample.
8	Hodowu, Korda & Ansong (2020)	Hybrid AES–ECC encryption	Two-level symmetric/asymmetric scheme that reduces cryptographic processing time and improves confidentiality and integrity of cloud data.	No fine-grained, attribute-based access control.
9	Cai & Yao (2022)	Symmetric-key encryption	Secure network data transmission combining encryption/decryption, dynamic key generation and shared-key update modules.	Targets data in transit rather than cloud-stored data.
10	Korda, Ansong & Hodowu (2021)	Homomorphic encryption (SDC)	Performs computations on scrambled cloud data without the client surrendering its secret key; assessed with big-O analysis and a Python implementation.	Evaluation limited to correctness and complexity analysis.
11	Akobre, Wiredu, Daabo & Agebure (2025)	RNS–AES-CBC with HMAC-SHA256	Hybrid scheme delivering confidentiality and integrity with encryption/decryption latencies of about 55–593 µs.	Benchmarked only on short (4–15 character) payloads.
12	Chillotti et al. (2020)	Fully homomorphic encryption (TFHE)	Fast bootstrapping enabling gate-by-gate evaluation of Boolean circuits on encrypted data.	Still far slower than computation on plaintext.
13	Chen et al. (2020)	Blockchain searchable public-key encryption (BSPEFB)	Replaces the central search server with a smart contract and provides forward and backward privacy.	Designed for cloud-assisted vehicular social networks.
14	Sahai & Waters (2005)	Fuzzy identity-based encryption	Treats identities as sets of descriptive attributes with error tolerance, founding ABE.	Supports only threshold policies.
15	Goyal et al. (2006)	KP-ABE	Associates access trees with user keys to achieve fine-grained access control over encrypted data.	Encryptor cannot choose who may decrypt.
16	Bethencourt, Sahai & Waters (2007)	CP-ABE	Embeds the access policy in the ciphertext so the data owner decides who can decrypt.	Security proven only in the generic group model.
17	Waters (2011)	CP-ABE	Expressive and efficient CP-ABE with security under standard (non-generic) assumptions.	Ciphertext size grows with policy size.
18	Emura et al. (2009)	Constant-ciphertext CP-ABE	Achieves constant ciphertext length and a constant number of pairing operations.	Restricted to AND-gate policies.

S/N	Author(s) (Year)	Focus / Technique	Key Contribution	Limitation / Gap
19	Yao, Chen & Tian (2015)	Lightweight ABE for IoT	Pairing-free KP-ABE built on elliptic-curve operations for resource-constrained devices.	Provides confidentiality only; no authentication.
20	Maji, Prabhakaran & Rosulek (2011)	Attribute-based signatures	Formalises ABS with signer privacy and unforgeability against colluding users.	No confidentiality of the signed data.
21	Zheng (1997)	Digital signcryption	Performs signing and encryption in one logical step at lower cost than sign-then-encrypt.	Not attribute-based; no fine-grained access control.
22	Liu, Huang & Liu (2015)	CP-ABSC for health records	Signcryption scheme for personal health records offering confidentiality, authenticity and signer privacy.	Later shown to fall short of claimed security (Rao, 2017).
23	Rao (2017)	CP-ABSC for health records	Improved CP-ABSC with public ciphertext verifiability, correcting weaknesses of earlier schemes.	Pairing-based; cost rises with the number of attributes.
24	Eltayieb et al. (2020)	Blockchain + ABSC	Combines blockchain and attribute-based signcryption for cloud data sharing without a trusted storage provider.	Shown to be insecure against confidentiality attacks (Li et al., 2022).
25	Li et al. (2022)	Cryptanalysis of blockchain ABSC	Demonstrates a confidentiality attack on the Eltayieb et al. (2020) scheme.	Highlights the need for formally verified blockchain–ABSC designs.
26	Nakamoto (2008)	Bitcoin blockchain	Peer-to-peer electronic cash using a proof-of-work, hash-chained public ledger without a trusted third party.	Limited throughput and high energy use.
27	Liang et al. (2017)	Blockchain data provenance (ProvChain)	Records immutable, timestamped provenance receipts for cloud data operations with low overhead.	Prototype evaluated in a single cloud storage setting.
28	Alkadi et al. (2021)	Blockchain + deep-learning IDS	BiLSTM-based collaborative intrusion detection with smart-contract support, evaluated on UNSW-NB15 and BoT-IoT.	Targets IoT/cloud networks rather than payment data.
29	Mercan et al. (2022)	Blockchain two-factor authentication	Uses a blockchain-based second factor to validate credit card transactions without a central third party.	Prototype-level evaluation.
30	Olorunshola, Okoroafor & Enem (2025)	Blockchain payment gateway (HappyPay)	Polygon-based gateway using smart contracts with MetaMask and WalletConnect integration.	Deployed on a test network only.

This synthesis suggests that payment platforms which clearly signal the strength of their underlying data-sharing mechanism to the customer — for instance, ranking platforms that adopt blockchain-integrated ABSC-type schemes above those relying on weaker encryption alone — could measurably reduce the customer's perceived risk at the point of an online transaction, and

consequently increase both purchase intention and trust, consistent with the perceived-risk and trust literature reviewed in Sections 3 and 4.

CONCLUSION

This review has examined the literature on cloud computing adoption in the payment card industry, cloud security issues and attack surfaces, the role of phishing in payment card fraud, the influence of perceived risk and fear of identity theft on online purchase intention and trust, and the cryptographic and blockchain-based techniques proposed to secure cloud-stored payment card data. The evidence reviewed indicates that no single cryptographic primitive — symmetric encryption, public-key encryption, searchable encryption, homomorphic encryption, ABE, or ABS in isolation — fully satisfies the combined requirement of confidentiality, integrity, availability, authenticity, and access control that cloud-based payment systems demand. Attribute-Based Signcryption, especially when integrated with blockchain to decentralize trust away from a single third-party provider, emerges from the literature as a promising technical direction for addressing the centralization, cost, and trust shortcomings of traditional cloud storage in the Payment Card Industry. However, because the leading blockchain-based ABSC scheme reviewed has been shown to be insecure against confidentiality attacks (Li et al., 2022), future work must prioritize constructions with rigorous security proofs and practical performance evaluation. If such schemes are adopted and their protections are clearly communicated to consumers, they have the potential to improve trust and willingness to conduct online transactions.

REFERENCES

Akobre, S., Wiredu, J. K., Daabo, M. I. & Agebure, M. A., 2025. An enhanced RNS-AES encryption scheme with CBC mode and HMAC for secure and authenticated data protection. Earthline Journal of Mathematical Sciences, 15(6), pp. 1091–1112.

Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S. & Rahman, M. S., 2019. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Generation Computer Systems, 95, pp. 511–521. https://doi.org/10.1016/j.future.2018.12.044

Alam, T., 2020. Cloud computing and its role in the information technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), pp. 108–115.

Ali, M., Khan, S. U. & Vasilakos, A. V., 2015. Security in cloud computing: Opportunities and challenges. Information Sciences, 305, pp. 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Alkadi, O., Moustafa, N., Turnbull, B. & Choo, K.-K. R., 2021. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE

Internet of Things Journal, 8(12), pp. 9463–9472. https://doi.org/10.1109/JIOT.2020.2996590

Banu, M. N. & Banu, S. M., 2013. A comprehensive study of phishing attacks. International Journal of Computer Science and Information Technologies, 4(6), pp. 783–786.

Bethencourt, J., Sahai, A. & Waters, B., 2007. Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy (SP'07). IEEE, pp. 321–334.

Boneh, D., Di Crescenzo, G., Ostrovsky, R. & Persiano, G., 2004. Public key encryption with keyword search. In: Advances in Cryptology – EUROCRYPT 2004, LNCS 3027. Berlin: Springer, pp. 506–522.

Cai, W. & Yao, H., 2022. A secure transmission method of network communication data based on symmetric key encryption algorithm. Wireless Personal Communications, 127, pp. 341–352. https://doi.org/10.1007/s11277-021-08266-w

Chen, B., Wu, L., Wang, H., Zhou, L. & He, D., 2020. A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks. IEEE Transactions on Vehicular Technology, 69(6), pp. 5813–5825. https://doi.org/10.1109/TVT.2019.2959383

Chen, C., Zhang, Z. & Feng, D., 2011. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In: Provable Security (ProvSec 2011), LNCS 6980. Berlin: Springer, pp. 84–101.

Chillotti, I., Gama, N., Georgieva, M. & Izabachène, M., 2020. TFHE: Fast fully homomorphic encryption over the torus. Journal of Cryptology, 33(1), pp. 34–91. https://doi.org/10.1007/s00145-019-09319-x

Delamaire, L., Abdou, H. & Pointon, J., 2009. Credit card fraud and detection techniques: A review. Banks and Bank Systems, 4(2), pp. 57–68.

El Alloussi, H., Fetjah, L. & Chaichaa, A., 2014. Securing the payment card data on cloud environment: Issues & perspectives. International Journal of Computer Science and Network Security, 14(11), pp. 14–20.

Eltayieb, N., Elhabob, R., Hassan, A. & Li, F., 2020. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. Journal of Systems Architecture, 102, p. 101653. https://doi.org/10.1016/j.sysarc.2019.101653

Emura, K., Miyaji, A., Nomura, A., Omote, K. & Soshi, M., 2009. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In: Information Security Practice and Experience (ISPEC 2009), LNCS 5451. Berlin: Springer, pp. 13–23.

Godfrey-Welch, D., Lagrois, R., Law, J., Anderwald, R. S. & Engels, D. W., 2018. Blockchain in payment card systems. SMU Data Science Review, 1(1), Article 3.

Goyal, V., Pandey, O., Sahai, A. & Waters, B., 2006. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, pp. 89–98.

Hille, P., Walsh, G. & Cleveland, M., 2015. Consumer fear of online identity theft: Scale development and validation. Journal of Interactive Marketing, 30, pp. 1–19. https://doi.org/10.1016/j.intmar.2014.10.001

Hodowu, D. K. M., Korda, D. R. & Ansong, E. D., 2020. An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using AES and ECC algorithm. International Journal of Engineering Research and Technology, 9(9), pp. 639–650.

Jordan, G., Leskovar, R. & Marič, M., 2018. Impact of fear of identity theft and perceived risk on online purchase intention. Organizacija, 51(2), pp. 146–155. https://doi.org/10.2478/orga-2018-0007

Kent, S. & Atkinson, R., 1998a. RFC 2401: Security Architecture for the Internet Protocol. Internet Engineering Task Force.

Kent, S. & Atkinson, R., 1998b. RFC 2402: IP Authentication Header. Internet Engineering Task Force.

Kim, J. & Lennon, S. J., 2013. Effects of reputation and website quality on online consumers' emotion, perceived risk and purchase intention. Journal of Research in Interactive Marketing, 7(1), pp. 33–56. https://doi.org/10.1108/17505931311316734

Korda, D. R., Ansong, E. D. & Hodowu, D. K. M., 2021. Securing data in the cloud using the SDC algorithm. International Journal of Computer Applications, 183, pp. 24–29. https://doi.org/10.5120/ijca2021921631

Li, J., Au, M. H., Susilo, W., Xie, D. & Ren, K., 2010. Attribute-based signature and its applications. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10). ACM, pp. 60–69. https://doi.org/10.1145/1755688.1755697

Li, X., Ge, L., Chen, J. & Peng, Z., 2022. Comments on 'A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud'. Journal of Systems Architecture, 131, p. 102702. https://doi.org/10.1016/j.sysarc.2022.102702

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K. & Njilla, L., 2017. ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid). IEEE, pp. 468–477. https://doi.org/10.1109/CCGRID.2017.8

Liu, J., Huang, X. & Liu, J. K., 2015. Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption. Future Generation Computer Systems, 52, pp. 67–76.

Madson, C. & Glenn, R., 1998a. RFC 2403: The Use of HMAC-MD5-96 within ESP and AH. Internet Engineering Task Force.

Madson, C. & Glenn, R., 1998b. RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH. Internet Engineering Task Force.

Maji, H. K., Prabhakaran, M. & Rosulek, M., 2011. Attribute-based signatures. In: Topics in Cryptology – CT-RSA 2011, LNCS 6558. Berlin: Springer, pp. 376–392.

Mell, P. & Grance, T., 2011. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Gaithersburg, MD: National Institute of Standards and Technology.

Mercan, S., Cebe, M., Akkaya, K. & Zuluaga, J., 2022. Blockchain-based two-factor authentication for credit card validation. In: Data Privacy Management, Cryptocurrencies

and Blockchain Technology (DPM 2021 / CBT 2021), LNCS 13140. Cham: Springer, pp. 319–327. https://doi.org/10.1007/978-3-030-93944-1_22

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. White paper. Available at: https://bitcoin.org/bitcoin.pdf

Nilson Report, 2022. Card fraud losses worldwide — 2021. The Nilson Report, December 2022. Available at: https://nilsonreport.com/articles/card-fraud-losses-worldwide/

Nilson Report, 2025. Payment card fraud losses approach $34 billion [Press release]. GlobeNewswire, 6 January 2025.

NIST (National Institute of Standards and Technology), 2001. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. Gaithersburg, MD: NIST.

Olorunshola, O. E., Okoroafor, C. D. & Enem, T. A., 2025. Leveraging the Polygon blockchain for a secured and transparent payment gateway. Asian Journal of Computer Science and Technology, 14(2), pp. 14–20. https://doi.org/10.70112/ajcst-2025.14.2.4358

Pham, V. V. H., Liu, X., Zheng, X., Fu, M., Deshpande, S. V., Xia, W., Zhou, R. & Abdelrazek, M., 2017. PaaS – black or white: An investigation into software development model for building retail industry SaaS. In: Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). IEEE, pp. 285–287.

Rao, Y. S., 2017. A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing. Future Generation Computer Systems, 67, pp. 133–151.

Rivest, R., 1992. RFC 1321: The MD5 Message-Digest Algorithm. Internet Engineering Task Force.

Rivest, R. L., Shamir, A. & Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), pp. 120–126.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. & Mohaisen, D., 2020. Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), pp. 1977–2008. https://doi.org/10.1109/COMST.2020.2975999

Sahai, A. & Waters, B., 2005. Fuzzy identity-based encryption. In: Advances in Cryptology – EUROCRYPT 2005, LNCS 3494. Berlin: Springer, pp. 457–473.

Singh, S., Jeong, Y.-S. & Park, J. H., 2016. A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications, 75, pp. 200–222.

Song, D. X., Wagner, D. & Perrig, A., 2000. Practical techniques for searches on encrypted data. In: Proceedings of the 2000 IEEE Symposium on Security and Privacy. IEEE, pp. 44–55.

Waters, B., 2011. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Public Key Cryptography – PKC 2011, LNCS 6571. Berlin: Springer, pp. 53–70.

Wood, G., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151, pp. 1–32.

Yao, X., Chen, Z. & Tian, Y., 2015. A lightweight attribute-based encryption scheme for the Internet of Things. Future Generation Computer Systems, 49, pp. 104–112.

Zhang, Y., Deng, R. H., Liu, X. & Zheng, D., 2021. Outsourcing service fair payment based on blockchain and its applications in cloud computing. IEEE Transactions on Services Computing, 14(4), pp. 1152–1166. https://doi.org/10.1109/TSC.2018.2864191

Zheng, Y., 1997. Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption). In: Advances in Cryptology – CRYPTO '97, LNCS 1294. Berlin: Springer, pp. 165–179.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H., 2017. An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85